



STIC Search Report

EIC 2100

STIC Database Tracking Number: 134723

TO: Baoquoc To
Location:
Art Unit : 2162
Tuesday, October 12, 2004

Case Serial Number: 09/832737

From: Geoffrey St. Leger
Location: EIC 2100
PK2-4B30
Phone: 308-7800

geoffrey.stleger@uspto.gov

Search Notes

Dear Examiner To,

Attached please find the results of your search request for application 09/832737. I searched Dialog's foreign patent files, technical databases, product announcement files and general files; along with the Internet.

Please let me know if you have any questions.

Regards,


Geoffrey St. Leger
4B30/308-7800
5718723540



STIC Search Results Feedback Form

EIC 2100

Questions about the scope or the results of the search? Contact **the EIC searcher or contact:**

Anne Hendrickson, EIC 2100 Team Leader
308-7831, CPK2-4B40.

Voluntary Results Feedback Form

➤ *I am an examiner in Workgroup:* *Example: 2133*

➤ *Relevant prior art found, search results used as follows:*

- 102 rejection
- 103 rejection
- Cited as being of interest.
- Helped examiner better understand the invention.
- Helped examiner better understand the state of the art in their technology.

Types of relevant prior art found:

- Foreign Patent(s)
- Non-Patent Literature
(journal articles, conference proceedings, new product announcements etc.)

➤ *Relevant prior art not found:*

- Results verified the lack of relevant prior art (helped determine patentability).
- Results were not useful in determining patentability or understanding the invention.

Comments:

Drop off or send completed forms to STIC/EIC2100 CPK2-4B40





STIC EIC 2100

Search Request Form

Jeff

Today's Date:

10/07/04

What date would you like to use to limit the search?

Priority Date: 06/06/2001 Other:

Name Tony Bao (VOC)

AU 2062 Examiner # 7889

Room # 4042 Phone 305-7649

Serial # 09/832737

Format for Search Results (Circle One):

PAPER DISK EMAIL

Where have you searched so far?

USP DWPI EPO JPO ACM IBM TDB
 IEEE INSPEC SPI Other

Is this a "Fast & Focused" Search Request? (Circle One) YES NO

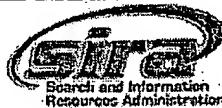
A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at <http://ptoweb/patents/stic/stic-tc2100.htm>.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

undo or revert the changes made to
the published page by changing the
files in the predetermined order

Article # Puklin 1996 Lotus note
reverted the changes by comparing the files
in 3 or 4 or 5 minutes.

STIC Searcher Geoffrey St. Leger Phone 308-7800
Date picked up 10/8/04 Date Completed 10/12/04



File 8: Ei Compendex(R) 1970-2004/Oct W1
 (c) 2004 Elsevier Eng. Info. Inc.
 File 35: Dissertation Abs Online 1861-2004/Sep
 (c) 2004 ProQuest Info&Learning
 File 202: Info. Sci. & Tech. Abs. 1966-2004/Sep 09
 (c) 2004 EBSCO Publishing
 File 65: Inside Conferences 1993-2004/Oct W2
 (c) 2004 BLDSC all rts. reserv.
 File 2: INSPEC 1969-2004/Oct W1
 (c) 2004 Institution of Electrical Engineers
 File 233: Internet & Personal Comp. Abs. 1981-2003/Sep
 (c) 2003 EBSCO Pub.
 File 94: JICST-EPlus 1985-2004/Sep W2
 (c) 2004 Japan Science and Tech Corp (JST)
 File 483: Newspaper Abs Daily 1986-2004/Oct 09
 (c) 2004 ProQuest Info&Learning
 File 6: NTIS 1964-2004/Oct W1
 (c) 2004 NTIS, Intl Cpyrht All Rights Res
 File 144: Pascal 1973-2004/Oct W1
 (c) 2004 INIST/CNRS
 File 434: SciSearch(R) Cited Ref Sci 1974-1989/Dec
 (c) 1998 Inst for Sci Info
 File 34: SciSearch(R) Cited Ref Sci 1990-2004/Oct W1
 (c) 2004 Inst for Sci Info
 File 99: Wilson Appl. Sci & Tech Abs 1983-2004/Sep
 (c) 2004 The HW Wilson Co.
 File 583: Gale Group Globalbase(TM) 1986-2002/Dec 13
 (c) 2002 The Gale Group
 File 266: FEDRIP 2004/Jul
 Comp & dist by NTIS, Intl Copyright All Rights Res
 File 95: TEME-Technology & Management 1989-2004/Jun W1
 (c) 2004 FIZ TECHNIK
 File 438: Library Lit. & Info. Science 1984-2004/Sep
 (c) 2004 The HW Wilson Co
 File 256: TecInfoSource 82-2004/Jul
 (c) 2004 Info.Sources Inc

Set	Items	Description
S1	199194	(DETECT??? OR NOTIC??? OR SPOT? ? OR SPOTTED OR SPOTTING OR SENS??? OR RECOGNI?) (7N) (CHANG??? OR ALTER??? OR ALTERATION? ? OR MODIF???? OR MODIFICATION? ? OR EDIT??? OR DELET??? OR E- RAS??? OR REMOV??? OR RENAM??? OR VANDALISM OR DEFAC?)
S2	79165	(MASTER OR ORIGINAL OR PRIMARY OR MAIN) (10N) (REPLAC? OR RE- STOR??? OR OVERWRIT? OR REVERT??? OR REVERSION OR SWAP???? OR SUBSTITUT? OR SWITCH??? OR EXCHANG??? OR FIX??? OR CORRECT???)
S3	1211	S2(5N) (AUTOMAT? OR DYNAMIC? OR REAL() TIME OR BEHIND(2W) SCE- NE? ? OR TRANSPARENT? OR FLY)
S4	11	S1 AND S3
S5	7	RD (unique items)
S6	444	S1 AND S2
S7	1	S6 AND (WEBPAGE? ? OR (WEB OR INTERNET) () (PAGE? ? OR SITE? ?) OR WEBSITE? ?)
S8	15	WEBAGAIN
S9	333	S1 AND (WEBPAGE? ? OR (WEB OR INTERNET) () (PAGE? ? OR SITE? ?) OR WEBSITE? ?)
S10	15	S9 AND (HACK??? OR DEFAC? OR VANDALISM)
S11	156	S2 AND (WEBPAGE? ? OR (WEB OR INTERNET) () (PAGE? ? OR SITE? ?) OR WEBSITE? ?)
S12	8	S11 AND (HACK??? OR DEFAC??? OR VANDALISM)
S13	23	S10 OR S12

13/5/1 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2003 EBSCO Pub. All rts. reserv.

00692906 03SR08-012

Web security -- Protecting your company's Web site from all kinds of defacement is crucial, so products which can help are vital to your security...

Marshall, Geoff
SC/Info Security News Magazine , August 1, 2003 , v14 n8 p66-71, 5
Page(s)

ISSN: 1096-7974
Company Name: Gillian Technologies; GFI Software USA; Network
Associates; Secuve; Tripwire
URL: <http://www.gillian.com> <http://www.gfi.com> <http://www.mcafeeb2b.com>
<http://www.secuve.com> <http://www.tripwire.com>
Product Name: G-Server; GFI LANguard System Integrity Monitor; McAfee
Entercept; Secuve TOS; Tripwire

Languages: English
Document Type: Buyer and Vendor Guide
Grade (of Product Reviewed): A; C; B; B; C
Geographic Location: United States

Presents a buyer's guide to Web server security solutions that safeguard against unauthorized changes to the site. Shows a table comparing seven products from seven vendors on **detection of changes**, prevention of **changes**, prevention of exposure of **defaced** content, automatic delivery of good content after **hack**, and tools to restore **Web site** after **hack**. Products reviewed and their rating on a scale of 1 to 5 are: G-Server (\$25,000) from Gillian Technologies - 5; GFI LANguard System Integrity Monitor (\$0) from GFI Software USA - 3; McAfee Entercept (\$7,885) from Network Associates - 4; Secuve TOS (\$10,000) from Secuve - 4; Tripwire (\$7,590) from Tripwire - 3; WatchGuard Applock/Web (\$629) from WatchGuard Technologies - 4; WebAgain (\$995) from Lockstep Systems - 3. Reports that G-Server is ``Best Buy'' while McAfee Entercept merits ``Recommended.'' Includes a table, three photos, and three product summaries. (MEM)

Descriptors: Web Server; Security; **Web Sites**; Web Publishing;
Security Measures; Web Management; Web Tools

Identifiers: G-Server; GFI LANguard System Integrity Monitor; McAfee
Entercept; Secuve TOS; Tripwire; Gillian Technologies; GFI Software USA
; Network Associates; Secuve; Tripwire

13/5/2 (Item 2 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2003 EBSCO Pub. All rts. reserv.

00614817 00IK11-203

The joke is on the vandals -- Lockstep's WebAgain 2.0 will notify you of hacks so you can sit back and relax

Rohan, Rebecca
InternetWeek , November 20, 2000 , n838 p48, 56, 2 Page(s)

ISSN: 0746-8121
Company Name: Lockstep Systems
URL: <http://www.lockstep.com>
Product Name: WebAgain
Languages: English
Document Type: Software Review
Grade (of Product Reviewed): B
Geographic Location: United States

Presents a favorable review of WebAgain (\$995), a security utility from Lockstep Systems of Scottsdale, AZ (877). Explains that it **detects** unauthorized **changes** to **Web sites** on a schedule that the administrator chooses and restores vandalized **Web pages** around the clock. Highlights its ease of use; remote functionality; ease of installation; and notification of changes via Simple Mail Transfer Protocol (SMTP) mail, as an entry in the NT Event Log on any computer in the network, or via a Simple Network Management Protocol (SNMP) Trap of what it found and repaired. Mentions, however, that in order to see properties for

files in the archive, the user must click on only one file and look at a bar below the file list. Concludes that it represents a smart way to protect corporate investments in the **Web site** and the organizational image. Includes two sidebars, two screen displays, and a product summary. (MEM)

Descriptors: Security; Web Management; Utility Program; Web Tools; Disaster Recovery; Remote Computing; Enterprise Computing
Identifiers: WebAgain; Lockstep Systems

13/5/3 (Item 1 from file: 483)

DIALOG(R)File 483:Newspaper Abs Daily
(c) 2004 ProQuest Info&Learning. All rts. reserv.

07671364 SUPPLIER NUMBER: 677048811
WEBSITE **VANDALS HIT BOOK ON KERRY** ; HACKERS **TARGET CRITICAL TOME**
Bray, Hiawatha
Boston Globe, p C.2
Aug 11, 2004
ISSN: 0743-1791 NEWSPAPER CODE: BOST
DOCUMENT TYPE: News; Newspaper article
LANGUAGE: English RECORD TYPE: ABSTRACT

ABSTRACT: Yesterday, someone managed a more aggressive alteration at the Barnes & Noble.com site. This time, the photo of the book's jacket, featuring an older (John F. Kerry), was replaced with a photo of Kerry as a young man in Vietnam, surrounded by fellow servicemen. And the book's title was changed to "Fit For Command." Within hours, Barnes & Noble had **restored** the **original** jacket photo.

DESCRIPTORS: **Vandalism** ; Computer security; Presidential elections; Political campaigns; Books-titles -- Unfit For Command; Computer crime; **Web sites**
NAMED PERSONS: Kerry, John F
GEOGRAPHIC NAMES: United States; US
COMPANY INFORMATION:
Regnery Publishing Inc NAICS: 511130

13/5/4 (Item 2 from file: 483)

DIALOG(R)File 483:Newspaper Abs Daily
(c) 2004 ProQuest Info&Learning. All rts. reserv.

07373950 SUPPLIER NUMBER: 382803701
Jolted Over Electronic Voting; Report's Security Warning Shakes Some States' Trust
Schulte, Brigid
Washington Post, p A.01
Aug 11, 2003
ISSN: 0190-8286 NEWSPAPER CODE: TWP
DOCUMENT TYPE: News; Newspaper article
LANGUAGE: English RECORD TYPE: ABSTRACT

ABSTRACT: Maryland officials, who signed a \$55.6 million agreement with Diebold for 11,000 touch-screen voting machines just days before the Hopkins report came out, have asked an international computer security firm to review the system's security. If they don't like what they find, officials have said, the sale will be off. [Avi Rubin] analyzed portions of Diebold software source code that was mistakenly left on a public **Internet site** and concluded that a teenager could manufacture "smart" cards and vote several times. Further, he said, insiders could program the machine to **alter** election results without **detection**. All machines had the same password hard-wired into the code. And in some instances, it was set at 1111, a number laughably easy to **hack**, Rubin said. That doesn't satisfy some critics. "The most important thing about the Hopkins report is not the security holes they found, but irrefutable proof that all this stuff that the machines are secure is hot air," said David Dill, a computer scientist at Stanford University who has turned the debate over electronic

machines into a national crusade.

DESCRIPTORS: Computer upgrading; Voting machines; Computer security
GEOGRAPHIC NAMES: States-US

13/5/5 (Item 3 from file: 483)
DIALOG(R) File 483:Newspaper Abs Daily
(c) 2004 ProQuest Info&Learning. All rts. reserv.

06208544 SUPPLIER NUMBER: 62830745

Office Hours: WPM

Phipps, Claire

Guardian, p OFFICE.3

Oct 23, 2000

ISSN: 0261-3077 NEWSPAPER CODE: MG

DOCUMENT TYPE: Commentary; Newspaper article

LANGUAGE: English RECORD TYPE: ABSTRACT

ABSTRACT: A piece in the most recent Harvard Business Review by Robert Goffee and Gareth Jones puts forward the theory that managers ought to decide upon a character flaw to display when in the office. This, they say, has two advantages: it makes the boss seem more human and thus more approachable (true - WPM has always found jolly nice people ever so difficult to talk to); and it also serves the purpose of masking even more unsavoury character traits (a hint: it doesn't. We know them all). WPM can only wonder how bosses decide on the one fault they are prepared to reveal. "Shall I assemble all the paperclips in the office into a long chain? Hm, might not mask the fact that I'm a crashing bore. Set my computer to ping loudly when email arrives? No, need to be more human. Empty the photocopier of paper? A spot of **vandalism** in the staff toilets?" *There's no advice on how to deal with a pub rock-loving colleague on www.secretary1.com, but there is plenty of stuff about improving your shorthand, finding companies to make conference badges and hiring a massage therapist to come to your office, and so it is **website** of the week. Although WPM, whose desk is currently carpeted in sticky memo notes of every hue, is disconcerted to learn from the site that this method of information gathering could give the impression that WPM is disorganised .

DESCRIPTORS: Secretaries; Managers

13/5/6 (Item 4 from file: 483)
DIALOG(R) File 483:Newspaper Abs Daily
(c) 2004 ProQuest Info&Learning. All rts. reserv.

06020366 SUPPLIER NUMBER: 54944970

Computer Company Warns of 'Attack' Software

Bridis, Ted

Wall Street Journal, p B2

Jun 9, 2000

ISSN: 0099-9660 NEWSPAPER CODE: WSJ

; Newspaper article

LANGUAGE: English RECORD TYPE: ABSTRACT

ABSTRACT: The greatest threat is posed to e-commerce **Web sites**, which could be disrupted if "zombie" computers with the attack software were instructed to overwhelm those sites with floods of spurious data, called a "distributed denial of service" attack. The same technique, on an enormous scale, was used in February to bring down some of the Internet's marquee sites, including Yahoo!, CNN and eBay. But in those cases, **hackers** broke into corporate and academic computers to implant the attack software rather than tricking victims into implanting it themselves. The program appears to be a video file in the so-called avi format, but actually carries an "exe" extension, signifying that it will execute commands on the computer. The name of the infected file **changes** randomly to avoid easy **detection**, but typically includes nonsensical letters, such as "WUYILLKM."

13/5/7 (Item 5 from file: 483)
DIALOG(R)File 483:Newspaper Abs Daily
(c) 2004 ProQuest Info&Learning. All rts. reserv.

05929752 SUPPLIER NUMBER: 51977930
MAKER OF CYBER PATROL SETTLES WITH HACKERS WHO SPILLED SECRETS BUT ACLU ARGUES DEAL CAN'T BAR OTHERS
Bray, Hiawatha
Boston Globe, p E6
Mar 28, 2000
ISSN: 0743-1791 NEWSPAPER CODE: BG
DOCUMENT TYPE: ECO; Newspaper article
LANGUAGE: English RECORD TYPE: ABSTRACT

ABSTRACT: The controversy began when Eddy Jansson of Sweden and Matthew Skala of Canada deciphered the code that makes Cyber Patrol work. They then wrote a program called CPHack, which enables the user to read a complete list of all **Internet sites** blocked by Cyber Patrol. CPHack also reveals the **master** password for Cyber Patrol, so that a user can simply **switch** off the program, which filters out pornography and other objectionable material. Microsystems went to court, charging that Jansson and Skala had violated their copyright by creating and distributing CPHack. Last week, a federal judge in Boston, Edward Harrington, issued a temporary injunction against Jansson and Skala and their Internet service providers. The four defendants were ordered to stop posting CPHack on the Internet. They quickly complied.

13/5/8 (Item 6 from file: 483)
DIALOG(R)File 483:Newspaper Abs Daily
(c) 2004 ProQuest Info&Learning. All rts. reserv.

05812636 SUPPLIER NUMBER: 47258345
Viruses And Their Cures
Lewis, Peter H
New York Times, p 1
Dec 16, 1999
ISSN: 0362-4331 NEWSPAPER CODE: NY
DOCUMENT TYPE: Commentary; Newspaper article
LANGUAGE: English RECORD TYPE: ABSTRACT

ABSTRACT: Kathy Fithen, manager of the Computer Emergency Response Team at Carnegie Mellon University, a project that receives part of its financing from the Department of Defense, said: "We are anticipating a lot of date-triggered viruses because of Jan. 1. This is really a time to be diligent" in following standard antivirus procedures, Ms. Fithen said, "but it's not a time for panic." The team maintains a computer security **Web page** at www.cert.org/y2k-info. Several of the newer threats, including viruses called Prilissa and Mypics, are scheduled to do their nastiest work in coming weeks, in Prilissa's case when someone opens an infected e-mail attachment on Christmas Day, and when Mypics **detects** the computer's clock **changing** to 2000. Other viruses are expected to emerge in coming weeks as their twisted creators try to capitalize on Y2K-related confusion. Some of these viruses can reformat your hard disk drive, permanently erasing all the files on it. Some can mail themselves to your friends and associates by commandeering your e-mail address book. There is even one that can alter your system and notify the **hacker** via e-mail when your computer is vulnerable to further attacks.

DESCRIPTORS: Computer viruses; Year 2000; Computer programming; Emergency preparedness
CODEN: NYTIAO

13/5/9 (Item 7 from file: 483)
DIALOG(R)File 483:Newspaper Abs Daily

04368981

Air Force Computer Invaded As Hackers Forge Web Page
Schiessel, Seth
New York Times, Sec D, p 18, col 1
Dec 31, 1996
ISSN: 0362-4331 NEWSPAPER CODE: NY
DOCUMENT TYPE: News; Newspaper
LANGUAGE: English RECORD TYPE: ABSTRACT
LENGTH: Long (18+ col inches)

ABSTRACT: At least one computer **hacker** broke into the Air Force's main World Wide Web computer on Dec 29, 1996, **replacing** the service's home page with obscenities and anti-government slogans, an Air Force spokesman said on Dec 30.

DESCRIPTORS: Computer crime; **Hackers** ; **Web sites** ; Internet

COMPANY INFORMATION:

Air Force-US

13/5/10 (Item 1 from file: 6)

DIALOG(R)File 6:NTIS

(c) 2004 NTIS, Intl Cpyrgh All Rights Res. All rts. reserv.

2031074 NTIS Accession Number: PB97-503395/XAB

Data Grabber Web Site Security (on CD-ROM)
(Software)

CyberVista, Inc. San Mate, CA.

Corp. Source Codes: 114005000

Jul 97 1 CD-ROM

1996

Languages: English

Journal Announcement: GRAI9801

Requires Windows 3.1, 95, or NT. See also PB97-503387 and PB97-503445.

The software is on a disc. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703) 605-6000 (other countries); fax at (703) 321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.

NTIS Prices: CD-ROM \$495.00

Country of Publication: United States

This product provides security for a user's **web site** by automatically and without attendance, monitoring the site. It automatically and without attendance restores a **hacked web site** and notifies the **web site** administrator. It also retains **hacked** version copies. It automatically, and without personal attendance, **restores** a **web site**, that has been tampered with, to its **original** condition, and automatically notifies the **web site** administrator via e-mail or alphanumeric paging of the restoration status. The user specifies the **web site** and the frequency of unattended monitoring. It uses Cyber Vista's Data Grabber technology to automatically, and without personal attendance, monitor the specified **web site** for unauthorized changes such as **hacked** graphic images, **hacked** text, etc. It automatically retains a copy of the **hacked** version of the **web site**.

Descriptors: World Wide **Web** ; * **Sites** ; *Computer security; Computer networks; Computer program integrity; Computer information security; Computer architecture; Data base management systems; Systems engineering; Computer communications; Computer graphics; Monitoring

Identifiers: Network security; **Hackers** ; NTISCVVIS

Section Headings: 88A* (Library and Information Sciences--Operations and Planning); 88B (Library and Information Sciences--Information Systems); 62B* (Computers, Control, and Information Theory--Computer Software); 45C* (Communication--Common Carrier and Satellite)

13/5/11 (Item 1 from file: 144)

DIALOG(R)File 144:Pascal

(c) 2004 INIST/CNRS. All rts. reserv.

16810017 PASCAL No.: 04-0467559
Co-operative monitor web page based on MD5
GCC 2003 : grid and cooperative computing : Shanghai, 7-10 December 2003,
revised papers

GUOHUN ZHU; YUQING MIAO

MINGLU LI, ed; XIAN-HE SUN, ed; QIANNI DENG, ed; JUN NI, ed
Guilin Institute of Electronic Technology, 541004 Guilin, China
Grid and cooperative computing. International workshop, 2 (Shanghai CHN)

2003-12-07

Journal: Lecture notes in computer science, 2004, 3032 179-182

ISBN: 3-540-21988-9 ISSN: 0302-9743 Availability: INIST-16343;
354000117866892080

No. of Refs.: 8 ref.

Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)

Country of Publication: Germany

Language: English

This paper presents a new approach to **detect defacement** of the **web page** and have it back up in real-time. The mechanism base on integrity verified in a host and co-operative validated among a group of **web sites**. All upload page and data by legitimate user would be generated a digest file and copy to a backup directory. Monitor process not only audit collected the **web page**, but also interval exchange the **web page** audit index with adjoin node. While **hacker defaced** the **web page**, the monitor process will alarm master and recover page, also send a message to another web service. Lastly, the performance presented by contract with some utility tools.

English Descriptors: Distributed computing; Grid; Internet; Real time; Integrity; **Web site** ; Alarm; World wide web; Audit; Delinquency; Contract; Web service

French Descriptors: Calcul reparti; Grille; Internet; Temps reel; Integrite ; Site Web; Alarme; Reseau web; Audit; Delinquance; Contrat; Service web

Classification Codes: 001D02B04

Copyright (c) 2004 INIST-CNRS. All rights reserved.

13/5/12 (Item 1 from file: 34)

DIALOG(R)File 34:SciSearch(R) Cited Ref Sci
(c) 2004 Inst for Sci Info. All rts. reserv.

12832473 Genuine Article#: BAC97 Number of References: 5

Title: **Co-operative monitor web page based on MD5**

Author(s): Zhu GH (REPRINT) ; Miao YQ

Corporate Source: Guilin Inst Elect Technol,Guilin 541004//Peoples R China/
(REPRINT); Guilin Inst Elect Technol,Guilin 541004//Peoples R China/
, 2004, V3033, P179-182

ISSN: 0302-9743 Publication date: 20040000

Publisher: SPRINGER-VERLAG BERLIN, HEIDELBERGER PLATZ 3, D-14197 BERLIN,
GERMANYGRID AND COOPERATIVE COMPUTING, PT 2

Series: LECTURE NOTES IN COMPUTER SCIENCE

Language: English Document Type: ARTICLE

Geographic Location: Peoples R China

Abstract: This paper presents a new approach to **detect defacement** of the **web page** and have it back up in real-time. The mechanism base on integrity verified in a host and co-operative validated among a group of **web sites**. All upload page and data by legitimate user would be generated a digest file and copy to a backup directory.

Monitor process not only audit collected the **web page**, but also interval exchange the **web page** audit index with adjoin node. While **hacker defaced** the **web page**, the monitor process will alarm master and recover page, also send a message to another web service.

Lastly, the performance presented by contract with some utility tools.

Cited References:

ALVESFOSS J, 1995, P94, P INT SOC 1995 S NET
ANDERSON JP, 1980, COMPUTER SECURITY TH
BACE RG, 2000, INTRUSION DETECTION
BRAUE D, INTRUSION DETECTION
ZHU GH, 2002, P350, P CROSS STRAIT INF T

13/5/13 (Item 1 from file: 583)
DIALOG(R)File 583:Gale Group Globalbase(TM)
(c) 2002 The Gale Group. All rts. reserv.

09575666
e-Cop.net sets CIA on **website defacers**
MALAYSIA: NEW APPLICATION UNVEILED BY E-COP
The Star (XAT) 07 Aug 2001 In-Tech p.55
Language: ENGLISH

In Malaysia, a new application called Content Integrity Agent (CIA) has been introduced by e-Cop.net Surveillance Sdn Bhd (e-Cop), an Internet security service provider in Malaysia. This application will **detect** any unauthorised **modification** in **web site** and alert the company's Global Command Centre in order to overcome the intrusion. This will avoid any **defacement** caused by irresponsible **hackers**.

COMPANY: E-COP.NET SURVEILLANCE; INTERNET

PRODUCT: Computer & Data Security Software (7372CD); Database Vendors (7375);
EVENT: Product Design & Development (33);
COUNTRY: Malaysia (9MAO);

13/5/14 (Item 2 from file: 583)
DIALOG(R)File 583:Gale Group Globalbase(TM)
(c) 2002 The Gale Group. All rts. reserv.

09562410
NSTB's **website** for Techmonth **defaced**
SINGAPORE: NSTB'S TECHMONTH **WEBSITE HACKED**
The Straits Times (XBB) 16 Jul 2001 p.H6
Language: ENGLISH

The Techmonth **website** of Singapore's National Science and Technology Board (NSTB) has been **hacked** into, allegedly by a group of five **hackers** who call themselves KKND, ph4nt4, raver, calvim and nessus. The site's **main webpage** has been **replaced** with another **webpage** with the words "Talita, te amo! muito", which means "Talita, I love you! very much!" in Portuguese. NSTB held Techmonth 2000 in September 2000 to promote local entrepreneurship.

COMPANY: NATIONAL SCIENCE & TECHNOLOGY BOARD; NSTB
EVENT: Product Standards (35);
COUNTRY: Singapore (9SIN);

13/5/15 (Item 1 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c) 2004 Info.Sources Inc. All rts. reserv.

01185507 DOCUMENT TYPE: Product
PRODUCT NAME: PC-cillin Internet Security (185507)

Trend Micro Inc (505871)
10101 N De Anza Blvd, 2nd Floor
Cupertino, CA 95014 United States
TELEPHONE: (408) 257-1500

RECORD TYPE: Directory

CONTACT: Sales Department

PC-cillin (TM) Internet Security, offered by Trend Micro (TM), allows users to protect computers, networks, and PDAs from viruses, **hackers**, and spam messages. The system includes firewall, virus **detection** and **removal**, URL filtering, parental control, and spyware deletion features. Its Damage Cleanup Services are triggered when viruses are identified. PC-cillin Internet Security automatically prevents infected computers from accessing networks, limiting the spread of viruses. The product includes wireless device protection features. It also prevents unauthorized users from monitoring Internet activity. The system also supports the creation of multiple security profiles. An evaluation version of PC-cillin Internet Security can be downloaded from the Trend Micro **Web site**.

DESCRIPTORS: E-Mail Utilities; Internet Content Filters; Internet Security; Network Administration; Network Software; Spam; System Monitoring; Viruses & Worms

HARDWARE: IBM PC & Compatibles; Pentium

OPERATING SYSTEM: Internet Explorer; Netscape; Windows; Windows NT/2000; Windows XP

PROGRAM LANGUAGES: Not Available

TYPE OF PRODUCT: Micro

POTENTIAL USERS: Cross Industry

PRICE: Available upon request; Internet trial available

OTHER REQUIREMENTS: 64MB RAM required

REVISION DATE: 20040219

13/5/16 (Item 2 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c)2004 Info.Sources Inc. All rts. reserv.

01005339 DOCUMENT TYPE: Product

PRODUCT NAME: WebAgain 2.1.2 (005339)

Lockstep Systems Inc (682764)
PO Box 1906
Scottsdale, AZ 85252-1906 United States
TELEPHONE: (480) 596-9432

RECORD TYPE: Directory

CONTACT: Sales Department

Lockstep Systems offers WebAgain (TM) 2.1.2, a **Web site** protection utility. Site managers can use WebAgain to ensure that they are notified of any changes to their sites and that the **original** content is **restored** easily if an intruder makes unauthorized additions or changes. Without a solution such as WebAgain, **hackers** can vandalize site pages with false prices and information, graffiti, and other misinformation. The system scans sites for evidence of **hacking**, then sends e-mail notices to administrators when an es. WebAgain 2.1.2 also makes it easy to store various revisions of site con ; and to harvest **Web site** files. Site managers can protect several sites wit ndows (R), Linux, or UNIX site, whether in-house or hosted. The system creates a **Web site** -specific rescue kit that makes it easy to restore an entire **Web site** from a content archive.

DESCRIPTORS: Backup Utilities; Data Recovery; Disaster Planning & Recovery; Electronic Publishing; File Security; Internet Security; Intrusion Detection; Network Administration; System Monitoring; Webmasters

HARDWARE: IBM PC & Compatibles; UNIX
OPERATING SYSTEM: Internet Explorer; Linux; Netscape; UNIX; Windows;
Windows NT/2000
PROGRAM LANGUAGES: Not Available
TYPE OF PRODUCT: Mini; Micro; Workstation
POTENTIAL USERS: Site Owners, Webmasters, Content Managers
PRICE: Available upon request; also available in an edition for service
providers

REVISION DATE: 20011130

13/5/17 (Item 3 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c)2004 Info.Sources Inc. All rts. reserv.

00139290 DOCUMENT TYPE: Review

PRODUCT NAMES: WebAgain 2.5 (005339)

TITLE: To protect and serve: Web content management software protects...
AUTHOR: Fielden, Tim
SOURCE: Federal Computer Week, v16 n17 p33(1) May 27, 2002
ISSN: 0893-052X
HOMEPAGE: <http://www.fcw.com>

RECORD TYPE: Review

REVIEW TYPE: Review

GRADE: A

Lockstep Systems' WebAgain 2.5, a Web content management intermediate server, gets excellent marks overall, especially for its ability to ensure that content is staged and saved before deployment on a **Web site**. The staging server queries the **Web site** at user-configurable intervals to determine if files have differences. If files are found to unsynchronized, contents and files are captured and isolated on the Lockstep server, and the **original** content is **restored**. The software adds an entry in a log and sends the administrator a message. Many other product provide similar features, including Tripwire for **Web Pages** and WatchGuard AppLock, but only WebAgain can claim self-healing abilities through content restoration without manual intervention. WebAgain 2.5 guards against concerted **hacker** attacks and is an excellent tool for eliminating the danger of accidental content corruption. WebAgain 2.5 also provides a useful audit trail for all modifications made to a **Web site**. If the user decides to deploy WebAgain 2.5, the only change to workflow is that content is published to the WebAgain server instead of directly to a Web server. New features in WebAgain 2.5 include better security through support for virtual private network (VPN) tunnels and virtual directories, faster performance, a Japanese version, and support for Microsoft Windows XP.

COMPANY NAME: Lockstep Systems Inc (682764)

SPECIAL FEATURE: Charts

DESCRIPTORS: Content Management; Electronic Publishing; **Web Site**
Design; Workflow

REVISION DATE: 20020830

13/5/18 (Item 4 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c)2004 Info.Sources Inc. All rts. reserv.

00138736 DOCUMENT TYPE: Review

PRODUCT NAMES: MSSP (Managed Security Service Providers) (845701)

TITLE: E-Travel Books With MSSP: Outsources security operations to...
AUTHOR: Chen, Anne
SOURCE: eWeek, v19 n20 p45(1) May 20, 2002

ISSN: 1530-6283
HOMEPAGE: <http://www.eweek.com>

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Geoff Teekema, CIO for e-Travel, discusses his decision to outsource some operations to a managed security services provider (MSSP). Teekema says the vendor hired, TruSecure, did a full-scale analysis of the **Web site** and e-Travel's data center, using security scanners to determine what type of malicious behavior a rogue employee or **hacker** could cause should they get in back of the company's firewall. All security policies and procedures were also analyzed to find out how e-Travel was monitoring its site, how it responded to possible **hack** attempts, and how it verified that no one tried to illegally gain access to data. After the security audit, Teekema made some **changes**, including installation of intrusion **detection** software and tightening of security procedures. e-Travel also gives TruSecure an image of its infrastructure, as well as a full list of software and hardware applications, and TruSecure monitors all software patch releases, alerting Teekema when a new patch must be installed. If e-Travel decides not to install a patch because of application incompatibility, for instance, IT managers must document the reason. Those security openings are then specifically addressed in the next security audit to make sure the missing patch has not created a vulnerability.

COMPANY NAME: Vendor Independent (999999)
DESCRIPTORS: Internet Security; MSP (Management Service Providers);
Outsourcing; Vulnerability Scanners; Webmasters
REVISION DATE: 20020830

13/5/19 (Item 5 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c)2004 Info.Sources Inc. All rts. reserv.

00131586 DOCUMENT TYPE: Review

PRODUCT NAMES: Robotics (830265); Electronics (834777)

TITLE: Tin Dogs
AUTHOR: Vitaliano, Franco
SOURCE: OPEN, v2 n5 p43(4) May 2001
ISSN: 1530-9495
HOMEPAGE: <http://www.openmagazine.net>

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Such companies as Sony, Honda, and NEC are pushing the consumer robotics market. Sony's robotic canine, AIBO ERS-210, uses a number of sensors, including a 100k pixel SMOS color camera, to interact with environments. AIBO ERS-210 develops complex behaviors, responding to stimulation, or the lack of it. Sony has not been forthcoming about the AIBO ERS-210's technology, and a **hacker** cult, represented at such **Web sites** as www.AIBOhack.com, has sprung up around the robot. One **Web site** features flowcharts tracking W01 AIBOLife software evolution. Another examines the ROM Demo AIBO and W02 Hello AIBO behavior and personality applications. **Hacking** aside, the AIBO Master Studio (AMS) application lets users edit AIBO's motions, lights, and sounds. Several actions can be combined using the application's Behavior Arranger feature. Other companies are marketing robots to consumers. Honda's ASIMO is a humanoid robot that stands four feet tall and weighs 100 pounds. It can navigate through rooms and climb stairs. Plug-ins will expand its behavior in the future. NEC's R100 taps PC-based **editing** software and offers directional hearing, **recognizing** and responding to voices and commands. Prices for consumer robots should plummet within the next five years.

COMPANY NAME: Vendor Independent (999999)
DESCRIPTORS: Artificial Intelligence; Electronics; Robotics
REVISION DATE: 20011030

13/5/20 (Item 6 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c)2004 Info.Sources Inc. All rts. reserv.

00131067 DOCUMENT TYPE: Review

PRODUCT NAMES: Tripwire for Web Pages 1.0 (050971)

TITLE: Trip up Web taggers: Tripwire for Web Pages meets the graffiti...

AUTHOR: Andress, Mandy
SOURCE: InfoWorld, v23 n23 p76(1) Jun 4, 2001
ISSN: 0199-6649
HOMEPAGE: <http://www.infoworld.com>

RECORD TYPE: Review

REVIEW TYPE: Review

GRADE: A

Tripwire's Tripwire for Web Pages 1.0, an Apache Web server module that 'scans your Web site 's files and automatically detects whether an intruder has defaced or modified those files,' gets excellent marks for affordability; scalability; ease of use; ease of installation and administration; customizable intrusion response; and protection of static and dynamic Web pages . TripWire for Web Pages 1.0 is compatible only with the Apache Web server and transparently automates protection of Web sites running the Apache Web server. TripWire 1.0 operates by creating an MD5 hash of the World Wide Web site files to be protected. When the Apache server sends a response to a HTTP 'get' request (which grabs content from URLs), the server checks the hash of the file being served against the has stored in the TripWire database looking for a match. If the hashes do not match, the server does not serve the page and launches the customizable intrusion response mechanism. TripWire can be altered to conduct specific actions when it sees a modification. Testers found installation very straightforward, and that TripWire also assists in protecting sites that use dynamic Web pages by ensuring the integrity of Java class files and Perl scripts.

PRICE: \$1095

COMPANY NAME: Tripwire Security Systems Inc (664677)
SPECIAL FEATURE: Charts
DESCRIPTORS: Apache; File Security; Firewalls; Internet Security;
Intrusion Detection; System Monitoring; Web Servers; Webmasters
REVISION DATE: 20011030

13/5/21 (Item 7 from file: 256)
DIALOG(R)File 256:TecInfoSource
(c)2004 Info.Sources Inc. All rts. reserv.

00130258 DOCUMENT TYPE: Review

PRODUCT NAMES: Digimarc ImageBridge (020893); SureSign (049069); SysCoP (049077); Batch It! (049085)

TITLE: Digital Copyright Control: Digital watermarks and Web spiders...
AUTHOR: Binder, Kate
SOURCE: Photo>Electronic Imaging, v44 n5 p24(3) May 2001
ISSN: 0146-0153
HOMEPAGE: <http://www.peimag.com>

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

BlueSpike's Giovanni, Digimarc's Digimarc ImageBridge, Alphatec's EIKONAmark, Signum Technologies' SureSign, MediaSec Technologies' SysCoP, and RedSoft's Batch It! are digital watermarking and World Wide Web spider products that can protect online images from unauthorized use. Digital watermarks embed images with marks that cannot be seen by the human eye. The marks are only visible with special viewing components, but some can be found by Web-searching software. ImageBridge automatically routes viewers and possible copyright infringers directly to the image owner's **Web site**, where the pictures can be purchased legally. EIKONAmark has some of the same types of features, including the AlphaCrawler Web search utility. EIKONAmark can also scan and **detect alterations** made to image and highlights **changed** areas in red. BlueSpike makes Giovanni software, which it now markets to the record industry (in which it wants to be the dominant watermarking-standard provider). However, Giovanni watermarks can also be embedded in image files with marks as tiny as 100/100 pixels. Giovanni is not fazed by JPEG compression or **hackers** attempting to erase or destroy a watermark. SureSign is a plug-in for Photoshop that embeds a watermark, and SysCoP is a Web spider. Shareware programs available are Fluid Vision Systems' Tranz Image Watermarking System for JPEG images and BatchIt! for JPEG, BMP, PCX, PNG, GIF, and TIFF formats.

COMPANY NAME: Digimarc Corp (629936); Signum Technologies Ltd (702536); MediaSec Technologies LLC (702501); iRedSoft Technology Inc (702528)
SPECIAL FEATURE: Screen Layouts Charts
DESCRIPTORS: Copyrights; Digital Rights Management; Electronic Publishing
REVISION DATE: 20010730

13/5/22 (Item 8 from file: 256)
DIALOG(R) File 256:TecInfoSource
(c)2004 Info.Sources Inc. All rts. reserv.

00127156 DOCUMENT TYPE: Review

PRODUCT NAMES: WebAgain 2.0 (005339)

TITLE: The Joke Is on the Vandals: Lockstep's WebAgain 2.0 will notify...
AUTHOR: Rohan, Rebecca
SOURCE: InternetWeek, v838 p48(2) Nov 20, 2000
ISSN: 0746-8121
HOMEPAGE: <http://www.internetwk.com>

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: A

Lockstep Systems' WebAgain 2.0 gets excellent marks for features that **detect alterations to Web sites**, running on a user-set schedule and restores damaged **Web pages** around the clock. The user's presence or hands-on actions are not required since WebAgain alerts users to **hacks** by Simple Mail Transfer Protocol (SMTP) mail, either as an entry in the NT Event Log on any networked computer or through a Simple Network Management Protocol (SNMP) trap of what was found and fixed. Users can view details by launching WebAgain's administrator interface from any Windows 98 or higher computer on the same network to which the NT/2000 machine that runs the WebAgain service is connected. Testers quickly installed Web Again, which runs in the background, and then installed a user-friendly administration interface. The administration interface has a side bar of four icons (Status, Archive, Quarantine, and Message Log), from which users can view different types of information in the main viewing area. WebAgain 2.0 works on local or remote **Web sites** as well those that are hosted. Single sites or mirrors are served. WebAgain 2.0's easy-to-use tools **detect** even the tiniest **changes to Web sites**. No site can be protected from every attack, so WebAgain 2.0's ability to alert users to

hacks and inadvertent file corruption offers a very savvy way to protect a site and the image of an organization.

PRICE: \$995

COMPANY NAME: Lockstep Systems Inc (682764)

SPECIAL FEATURE: Screen Layouts Charts

DESCRIPTORS: Computer Security; Content Management; File Security; IBM PC & Compatibles; Internet Security; System Monitoring; Webmasters;

Windows NT/2000

REVISION DATE: 20010228

13/5/23 (Item 9 from file: 256)

DIALOG(R)File 256:TecInfoSource

(c) 2004 Info.Sources Inc. All rts. reserv.

00122998 DOCUMENT TYPE: Review

PRODUCT NAMES: Linux (833916); Computer Security (830071)

TITLE: Open-Source Software Doesn't Have To Be Unsafe

AUTHOR: Rist, Oliver

SOURCE: Information Week, v776 p110(2) Mar 6, 2000

ISSN: 8750-6874

HOMEPAGE: <http://www.informationweek.com>

RECORD TYPE: Review

REVIEW TYPE: Product Analysis

GRADE: Product Analysis, No Rating

Users who wonder if the Linux open source operating system (OS) is as invulnerable to security breaches as UNIX can find out how to configure Linux to fend off destructive attacks. Among resources are the **Web sites** of Linux vendors and of the CERT Coordination Center, Linux Online, Planet IT Security Tech Center, and Sendmail Consortium. To make the most of Linux, users should regard the open-source model as a flexible OS with security advantages that become possible through the type of 'hardening' done on UNIX systems. For instance, UNIX can be made just about invulnerable when small applications are coded in a single function architecture and are linked via scripting. Source code is openly available, which means that security experts can get an application or OS' source code and alter it to meet their own needs and to provide iron-clad security. Network administrators can also take measures to secure a general purpose Linux server without closely examining source code. Samba is a good choice, since it allows Linux to imitate the file and print services of Windows NT and similar services, as well as domain name services. Samba communicates with NT and can **replace** an NT **primary** controller so that the administrator can eliminate many security loopholes in a combined Linux-NT installation. DNS services running on Linux improve performance but make large amounts of data available to **hackers** who gain entry to the DNS server. To begin securing a Linux installation, users can restrict access to the BIND server and provide information only to certain specified users.



Article Tools

Ads by G

[Furl this Article](#)[Print](#)[Send](#)[Subscribe to Publication](#)[Help](#)

Publications by Name

DDoS
Killer
Secure
networ
denial o
(DoS) a
attacks
www.maz

Select one

Web S
Securi

Get the
Forum'
of a We
Attack"
Paper.
www.foru

Publications by Topic

[Arts & Entertainment](#)

Elimin
Attack
Enterpr
applian
Unmatc
since 2
www.v-se

[Automotive](#)[Business & Finance](#)[Computers & Technology](#)[Health & Fitness](#)[Home & Garden](#)[News & Society](#)[Reference & Education](#)[Sports](#)

Gilian Technologies Ships the G-Server; First Web Content Security Solution with ExitControl; New Network Appliance 'Mitigates Hack Attacks' - Product Announcement

[Edge: Work-Group Computing Report](#), May 1, 2000

[New!] Save a personal copy of this article and quickly find it again with Furl.net. [Get started now.](#) (It's free.)

Preven
Flood
High P
Protect
Experts
White P
www.Top

Webmasters and site security officers may sleep better tonight, thanks to the introduction and release of the G-Server, the first Web content security and integrity system with new ExitControl technology. Developed and marketed by Gilian Technologies Inc., a Silicon Valley-based Internet infrastructure company (with credentials in Israeli cryptography and military communications security), the G-Server prevents accidental or intentional damage to Website data by transparently intercepting and replacing corrupt, altered or defaced content before it is released to the public.

Conten
partn

THC

The announcement was made at the Internet Security Conference Tuesday in San Jose, Calif., where the product is being shown in booth number 156-157.

"You cannot stop site penetrations by persons unknown. However, you can be certain that a defacement is never seen by the customer," Rafael Feitelberg, Redwood City-

based CEO of the two-year-old Web infrastructure company. "Last year, more than 5,000 Websites were seriously compromised. Security archives demonstrate these attacks are on the rise reaching more than 1,000 such incursions per month. These damaged sites had traditional security technology installed. The G-Server could have saved them."

In recent months, major defacements have occurred on the Websites of The New York Times, Symantec, Lloyd's of London, Yahoo, NASDAQ, Wired, ABC-TV, MSN and even venerated security companies, among thousands of others.

"No one is totally immune from the malicious intentions of obsessed hackers, and Web managers have typically had few tools in their arsenals with which to mitigate hack attacks," said Joshua Greenbaum, a principal with Enterprise Applications Consulting, an industry research firm based in Berkeley, Calif. "Gilian's new ExitControl technology can change the balance of power by enabling Web sites to guarantee that the content they publish from their sites is as hacker-proof as possible."

The G-Server is designed to offer content-rich sites high reliability and assurances that the data they publish is genuine. This is especially important to publishers whose Web content is their fundamental business.

"Websites' legal liability is increasing as users rely on published content for trading and other business purposes," Greenbaum added. "E-Commerce, news media, financial and equity trading sites can't afford to publish incorrect or altered data. It could put them out of business."

A beta user at a major Northeastern U.S. newspaper (who declined to be identified by name due to security policies) reported the G-Server not only maintains content integrity but enables them to more effectively manage the staging and production processes. "Before we had a mixed bag of methods to post new content, now with G-Server, the process has become streamlined and efficient." The Next Step in Content Assurance

Unlike traditional security devices -- such as firewalls and access controls -- the G-Server won't impede hostile penetrations but instead acts to ensure only genuine, authorized content is ever published by a Website. Gilian has developed proprietary, high-performance, patent-pending ExitControl technology. ExitControl is like a guard standing at the exit of a store checking each shopper's receipts where the G-Server compares all requested data with a digital signature unique to that data. If the requested content fails the test, the G-server replaces the corrupt data with a genuine copy and then dispatches the copy to the user.

"Our testing of the G-Server indicates the product lives up to its billing," said Jeff Mace, president of MaceLabs Corp., an independent product testing company. "The detection of altered content works well and the recovery mechanisms run as specified. Functionally speaking, the G-Server is stable and robust, especially for first generation product. The G-Server's unique technology of dealing with unwanted intruders will easily make this product a winner, if not a necessity, for any mission critical corporate site." Network Transparency and Digital Signing

The G-Server is a systems-level solution that resides on a network between the Internet and a Web server. Because it uses no IP address -- the numerical method by which Internet systems identify each other (much like telephone numbers) -- it is literally invisible as a network device and makes it extremely secure.

As new content and material is created for the site, the high-performance G-Server creates algorithmically coded digital signatures of the content thus making any alteration) forgery or defacement easy to detect and correct. Any change in content will break the digital signature. When a Web object is requested, an integrity check is made by the G-Server against the digital signature on file. Genuine content will be allowed to pass without any noticeable delay. If the content fails muster, the replacement content is instantly delivered. At the same time, the G-server sends an event alert to the appropriate contact by e-mail, pager or telephone noting where the problem resides.

Installation, Pricing and Availability

G-Server comes as an appliance pre-installed and tested on a Pentium III-class network server and pre-configured to the host network where it will be installed. Installation is plug-and-use and often takes less than an hour to install and test. Pricing for the G-Server in its primary configuration begins at \$54,000 and is available immediately.

Gilian Technologies Inc. is a Silicon Valley-based Internet infrastructure company with credentials in Israeli cryptography and military communications security. It is the global technology leader in exit control security and content integrity systems for commercial Websites. Based upon patent-pending ExitControl technology, Gilian's G-Server solution ensures that all Web content published is both authentic and authorized, thus preventing any defacement damage while maintaining high availability. The company is headquartered in Redwood City, Calif. and has offices in Boston, Mass. and in Israel. Gilian Technologies is located on the Web at: www.gilian.com.

COPYRIGHT 2000 EDGE Publishing

COPYRIGHT 2000 Gale Group

 [Furl it](#)

 [Print](#)

 [Send](#)

 [Subscribe](#)

 [IN](#) 

[FindArticles](#) · [Furl](#) · [Grub](#) · [LookListings](#) · [Net Nanny](#) · [WiseNut](#) · [Zeal](#)

©2004 LookSmart, Ltd. All rights reserved. - [About Us](#) · [Advertise with Us](#) · [Advertiser Log-in](#) · [Privacy Policy](#) · [Terms of Service](#)

NEWS RELEASE
For Immediate Release

[Close](#)

Company Contact: Karl Forster
 President
 Lockstep Systems, Inc.
KForster@Lockstep.com
 Phone +1.480.596.9432
 Fax +1.480.596.9195

Media Contact: Joe Waldygo
 President
 JW Communications, Inc.
JoeW@JW-Comm.com
 Phone +1.480.632.5055
 +1.480.632.5070

NEW WEB AGAIN™ SOLVES WEB SITE VANDALISM

Phoenix, Arizona USA, June 12, 2000 - - Lockstep Systems, Inc. today announced the release of WebAgain™ version 1.0. We patent-pending Windows utility that automatically fixes vandalized Web sites. It is available immediately and priced at \$499

WebAgain is designed to solve the problems associated with web site defacement by automating content verification, alteration and the correction process. It can detect any type of alteration, whether obvious or subtle, and correct it without any need for involvement. WebAgain provides round-the-clock web site defacement protection by systematically comparing an organization's web site data to an archive maintained at the WebAgain Server. WebAgain detects any differences between the public site and the archive; immediately re-publishing the appropriate files and restoring the web site to its original form.

The defacement of an organization's web site exposes visitors to misleading information until the unauthorized change is discovered. As the site grows in size, it becomes more difficult and time consuming to manually verify each page for accuracy and completeness. Web site hacks may be present and left unidentified for some time before they are discovered because it becomes impossible to continually check the integrity of each page. By automating the web site verification, alteration discovery and correction process, WebAgain minimizes the time that web site visitors would be exposed to misleading information.

"Internet presence companies rely heavily on their web sites, but these sites are very vulnerable. Anyone with Internet access can potentially alter a web site, to post misleading information or to redirect sales traffic," said Karl Forster, Lockstep's President. "WebAgain proactively ensures the integrity of a web site and gives Internet presence companies a tool which automatically corrects any unauthorized changes. WebAgain defeats the goal of the hacker by quickly republishing the altered web pages."

WebAgain complements the methods and tools companies use to publish their web sites. It accepts web content from all web software programs, such as Microsoft Front Page and Adobe's GoLive and PageMill. Web authors publish their files to the WebAgain Server where it archives the web content and publishes the pages to the company's public web sites and any associated mirrors. WebAgain guarantees delivery of the content to each desired target web site by queuing the content and routinely attempting to deliver this information to all sites until each has successfully received the data.

Highlights of WebAgain version 1.0 include the ability to:

- Automatically detect defacement and unauthorized web site changes.
- Quickly restore defaced web pages and return web site to original form.
- Receive web pages from any web authoring software program.
- Simultaneously publish to multiple sites and guarantee delivery.
- Archive web site content and store multiple revisions.
- Publish a web site back to "any-point-in-time."
- Send notices via e-mail, SNMP traps, or NT Event Log messages, when changes are detected and corrected.
- Quarantine defaced and changed web pages for off-line inspection.
- Protect multiple web sites and their mirrors using a single WebAgain Server.

WebAgain can protect web sites hosted by a company internally or at an Internet Service Provider (ISP). To protect a web site requires access to the site through a network or dial-up connection. WebAgain runs as a Windows NT / Windows 2000 Service and provides round-the-clock protection. The WebAgain Server software contains a built-in fault tolerant feature allowing the software to continue operation in the event of power loss or machine reboot. The WebAgain Server may be remotely administered using WebAgain Administrator software. A single installation of WebAgain can protect multiple web sites with the licensing of a multi-web-site key.

WebAgain System Requirements: WebAgain Server software runs as a Windows NT/2000 Service on an IBM PC/Compatible Windows NT 4.0 or Windows 2000; requires 5MB of hard disk space (not including extra storage to hold Web site archives); 16 MB RAM; Microsoft Internet Explorer 4.0 or Netscape Navigator/Communicator 4.0. The WebAgain Remote Administrator requires Windows 95, 98, NT 4.0 or Windows 2000; Microsoft Internet Explorer 4.0 or Netscape Navigator/Communicator 4.0.

WebAgain is available direct from Lockstep Systems, Inc. and is priced at \$499.00 US for a single license to protect one web associated mirrors. A 30-day, full-featured trial version may be downloaded from Lockstep's web site: <http://www.lockstep.com>. Pricing available upon request; inquiries welcome.

Lockstep Systems, Inc., a privately held corporation, was founded in 1998 to develop and market e-continuity software utility to ensure the integrity and continuity of electronic data for Internet presence companies. Lockstep Systems, Inc., P.O. Box Scottsdale, Arizona (AZ) 85252-1906 USA. Telephone +1.480.596.9432. Fax +1.480.596.9195. Toll-free (in USA) 1.877.WE (877.932.3497). Web site URL: <http://www.lockstep.com>. Questions and comments are welcome via e-mail addressed to info@lockstep.com.

Note to Editors: Lockstep Systems and WebAgain are trademarks of Lockstep Systems, Inc. All other products mentioned are and/or registered trademarks of their respective manufacturers.

###

US-PAT-NO: 5983277

DOCUMENT-IDENTIFIER: US 5983277 A

TITLE: Work group computing for electronic design automation

----- KWIC -----

Detailed Description Text - DETX (50):

Before entering into a discussion of possible file states from a local user's point of view, embodiments of version control (or revisions) will be discussed. Version control allows a user to preserve and restore previous versions of files which have been modified. In a single-user environment, this is useful to facilitate "backtracking" which is when the user wishes to "undo" a series of significant changes to a file. It is also useful to prevent accidental data loss. In a multi-user setting, it is useful for arbitrating access to shared files, so that two users may not accidentally edit the same file simultaneously.

US-PAT-NO: 6405219

DOCUMENT-IDENTIFIER: US 6405219 B2

See image for Certificate of Correction

TITLE: Method and system for automatically updating the version
of a set of files stored on content servers

----- KWIC -----

Detailed Description Text - DETX (39):

The logic steps to a block 172 where the Primary and Secondary global servers generate a content update container that includes a previous version of the set of source files for each local content server. The Primary and Secondary global servers copy the previous version of modified source files and restore removed source files from the previous version to at least one sub-directory on the local content servers. The logic flows to a block 174 where the Primary and Secondary global servers cause the version of the set of source files on each local content server to roll back by renaming the previous version of the set of source files included in the content update container copied to the a sub-directory on each local content server. Also, any version of the source files that are newer than the previous version are deleted at this time. Next, the logic advances to an end block and terminates.

File 275:Gale Group Computer DB(TM) 1983-2004/Oct 12
(c) 2004 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Oct 12
(c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Oct 12
(c) 2004 The Gale Group
File 16:Gale Group PROMT(R) 1990-2004/Oct 12
(c) 2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2004/Oct 12
(c) 2004 The Gale Group
File 624:McGraw-Hill Publications 1985-2004/Sep 20
(c) 2004 McGraw-Hill Co. Inc
File 15:ABI/Inform(R) 1971-2004/Oct 12
(c) 2004 ProQuest Info&Learning
File 647:CMP Computer Fulltext 1988-2004/Oct W1
(c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Sep W1
(c) 2004 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2004/Oct 11
(c) 2004 The Dialog Corp.
File 369:New Scientist 1994-2004/Oct W1
(c) 2004 Reed Business Information Ltd.
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 610:Business Wire 1999-2004/Oct 10
(c) 2004 Business Wire.
File 613:PR Newswire 1999-2004/Oct 10
(c) 2004 PR Newswire Association Inc

Set	Items	Description
S1	280892	(DETECT??? OR NOTIC??? OR SPOT? ? OR SPOTTED OR SPOTTING OR SENS??? OR RECOGNI?) (7N) (CHANG??? OR ALTER??? OR ALTERATION? ? OR MODIF???? OR MODIFICATION? ? OR EDIT??? OR DELET??? OR E- RAS??? OR REMOV??? OR RENAM??? OR VANDALISM OR DEFAC?)
S2	179075	(MASTER OR ORIGINAL OR PRIMARY OR MAIN) (10N) (REPLAC? OR RE- STOR??? OR OVERWRIT? OR REVERT??? OR REVERSION OR SWAP???? OR SUBSTITUT? OR SWITCH??? OR EXCHANG??? OR FIX??? OR CORRECT???)
S3	3669	S2(5N) (AUTOMAT? OR DYNAMIC? OR REAL() TIME OR BEHIND(2W) SCE- NE? ? OR TRANSPARENT? OR FLY)
S4	36	S1(30N)S3
S5	18	RD (unique items)

5/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02603310 SUPPLIER NUMBER: 85903490 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Lockstep releases new version of WebAgain. (Security Tools). (WebAgain 2.5) (Brief Article) (Product Announcement)
Computers in Libraries, 22, 5, 55(2)
May, 2002
DOCUMENT TYPE: Brief Article Product Announcement ISSN: 1041-7915
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 151 LINE COUNT: 00017

WebAgain protects Web site content by automatically detecting unauthorized changes and automatically restoring the original content without human intervention. According to the company, additions and enhancements to version 2.5...

5/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02497001 SUPPLIER NUMBER: 73552068 (USE FORMAT 7 OR 9 FOR FULL TEXT)
TURNKEY SECURITY -- SmartGuard VPN Gateway offers secure turnkey tunnels between LANs. (Software Review) (Evaluation)
Glass, Brett
InternetWeek, 23
April 23, 2001
DOCUMENT TYPE: Evaluation ISSN: 1096-9969 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 1498 LINE COUNT: 00123

... Windows 2000 or Windows ME-at least for the moment. Both of these operating environments detect the changed files and attempt to restore the original WSOCK32.DLL file automatically. V-One told us that it's now developing ways around this problem.

Share The...

5/3,K/3 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02472796 SUPPLIER NUMBER: 69242103 (USE FORMAT 7 OR 9 FOR FULL TEXT)
WebAgain 2.0 Defeats Web Site Vandalism. (Brief Article) (Product Announcement)
Computers in Libraries, 21, 1, 12
Jan, 2001
DOCUMENT TYPE: Brief Article Product Announcement ISSN: 1041-7915
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 176 LINE COUNT: 00017

... publicly posted files to the most recent copy stored in the WebAgain Archive. When unauthorized changes are detected, WebAgain automatically restores the original content, quarantines a copy of the hack, and sends notification to the administrator, without taking...

5/3,K/4 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02412603 SUPPLIER NUMBER: 62956467 (USE FORMAT 7 OR 9 FOR FULL TEXT)
E-Business -- Lockstep Systems WebAgain 1.0. (Brief Article) (Product Announcement)
Network Computing, 40
June 26, 2000

DOCUMENT TYPE: Brief Article Product Announcement
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 146 LINE COUNT: 00015

ISSN: 1046-4468

TEXT:

...sites. The program continuously monitors a site, comparing content with archived pages. When the program **detects** unauthorized **alterations**, it **automatically restores** the **original** pages. In addition, when a problem does occur, notices (via e-mail or NT Event...

5/3,K/5 (Item 5 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01376577 SUPPLIER NUMBER: 09431139 (USE FORMAT 7 OR 9 FOR FULL TEXT)
New equipment standards will protect central offices. (telephone companies)
(includes a related article about CO modifications versus redesign)
Merritt, Richard; Muller, Nathan J.
Telephony, v219, n12, p30(3)
Sept 10, 1990
ISSN: 0040-2656 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1456 LINE COUNT: 00115

... country are taking a number of specific steps to prevent future CO disasters. **PHYSICAL PLANT MODIFICATIONS** * Install more reliable heat and smoke **detectors**, as well as **master** power **switches** * Relocate **automatic** sprinkler systems away from electrical equipment and route telephone and power cables in separate trays...

5/3,K/6 (Item 1 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2004 The Gale Group. All rts. reserv.

02858603 Supplier Number: 73226124 (USE FORMAT 7 FOR FULLTEXT)
Mobile Automation 2000 Named a 2001 Finalist by Network Computing for Well-Connected Award.
Business Wire, p0038
April 16, 2001
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 687

...
Automated discovery and automated hardware/software inventory (WMI, DMI, and
WFM support)

-- Remote event scheduling

-- **Detection** and prevention of unauthorized end-user **modification** to desktops
and critical configuration files

-- File-gathering and distribution mechanisms

-- **Automated replacement** of improperly modified files with the
original version

-- Web-based interface for diagnosing mobile system problems from anywhere,
including a wireless handheld...

5/3,K/7 (Item 2 from file: 621)
DIALOG(R)File 621:Gale Group New Prod.Annou.(R)
(c) 2004 The Gale Group. All rts. reserv.

02848715 Supplier Number: 72676882 (USE FORMAT 7 FOR FULLTEXT)
UGS Implements Mobile Automation 2000 for Worldwide Software Distribution and License Tracking.
Business Wire, p0166
April 3, 2001
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 611

... Automated discovery and automated hardware/software inventory (WMI, DMI and WFM support)

- Remote event scheduling
- **Detection** and prevention of unauthorized end-user **modification** to desktops and critical configuration files
- File-gathering and distribution mechanisms
- **Automated replacement** of improperly modified files with the **original** version

-- Web-based interface for diagnosing mobile system problems from anywhere, including a wireless handheld...

5/3,K/8 (Item 3 from file: 621)
DIALOG(R) File 621:Gale Group New Prod.Annou. (R)
(c) 2004 The Gale Group. All rts. reserv.

02183297 Supplier Number: 55879929 (USE FORMAT 7 FOR FULLTEXT)
Serena Software Delivers First eHealing Solution for the Enterprise.
Business Wire, p0221
Sept 28, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1044

... profile that is compared to a fingerprint generated on a problem desktop, laptop, or server. **Detect +Resolve** instantly identifies where **changes** have occurred and **automatically restores** the **original**, stable configuration. **Detect+Resolve** **restores** only the necessary components instead of reinstalling an entire application to preserve end user customizations...

5/3,K/9 (Item 1 from file: 636)
DIALOG(R) File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

05407626 Supplier Number: 93955654 (USE FORMAT 7 FOR FULLTEXT)
Fighting cyberterrorism. (Crime).
Information Systems Auditor, p3
Nov, 2002
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 227

... an additional level of security by providing organizations with a quick and automatic method to **detect** certain forms of cyberterrorism and other malicious **alterations** of their web or network server, the developer said. If an unauthorized **change** is **detected**, it will instantly notify the system administrator and **automatically restore** the web page or file back to its **original** state. This so-called "self-

5/3,K/10 (Item 2 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

03697304 Supplier Number: 47977262 (USE FORMAT 7 FOR FULLTEXT)
TEKTRONIX: CNN International links with Tektronix for new \$1 million+ multi-channel MPEG2 project
M2 Presswire, pN/A
Sept 15, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 466

... part of the CNNI channel operation which currently employs an LMS system and traditional tape **editing** to customize **spot** playback and programming for international markets. The entire system will operate under the control of ProBel **automation** and utilize existing Grass Valley **master control switchers**.

According to Gordon Castle: "Tektronix was selected as CNNI's partner because the Profile fit nicely..."

5/3,K/11 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

09724080 SUPPLIER NUMBER: 19750462 (USE FORMAT 7 OR 9 FOR FULL TEXT)
CNN International Links With Tektronix for New \$1 million+ (US) Multi-channel MPEG2 Project
PR Newswire, p912SFF020
Sep 12, 1997
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 485 LINE COUNT: 00046

... part of the CNNI channel operation which currently employs an LMS system and traditional tape **editing** to customize **spot** playback and programming for international markets. The entire system will operate under the control of ProBel **automation** and utilize existing Grass Valley **master control switchers**.

According to Gordon Castle, "Tektronix was selected as CNNI's partner because the Profile fit..."

5/3,K/12 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

00599568 92-14741
FreeHand's Move to Windows a Success
Heck, Mike
InfoWorld v14n8 PP: 63, 67 Feb 24, 1992
ISSN: 0199-6649 JRNL CODE: IFW
WORD COUNT: 2058

...TEXT: and ellipse.

FreeHand lets you backtrack over lines as you draw to make on-the- **spot alterations** . Other advanced **editing** features include the ability to retract a point's handle (which straightens the path segment) or **restore automatic curvature** (which returns an object to its **original symmetrical shape**).

By using the layering feature, you can make layers temporarily invisible and restrict...

5/3,K/13 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2004 CMP Media, LLC. All rts. reserv.

01235625 CMP ACCESSION NUMBER: INW20010423S0038
TURNKEY SECURITY - SmartGuard VPN Gateway offers secure turnkey tunnels
between LANs

Brett Glass
INTERNETWEEK, 2001, n 858, PG23
PUBLICATION DATE: 010423
JOURNAL CODE: INW LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: NETWORK MANAGEMENT
WORD COUNT: 1408

... Windows 2000 or Windows ME-at least for the moment. Both of these operating environments **detect** the **changed** files and attempt to **restore** the **original** WSOCK32.DLL file **automatically**. V-One told us that it's now developing ways around this problem.

Share The...

5/3,K/14 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2004 CMP Media, LLC. All rts. reserv.

01218309 CMP ACCESSION NUMBER: NWC20000626S0013
E-Business - Lockstep Systems WebAgain 1.0
NETWORK COMPUTING, 2000, n 1112, PG40
PUBLICATION DATE: 000626
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: New and Improved
WORD COUNT: 134

TEXT:

... sites. The program continuously monitors a site, comparing content with archived pages. When the program **detects** unauthorized **alterations**, it **automatically** **restores** the **original** pages. In addition, when a problem does occur, notices (via e-mail or NT Event...).

5/3,K/15 (Item 1 from file: 810)
DIALOG(R)File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0363662 BW660

CPI: CPI announces IMAGE-IN POWER PACK 3.2, Professional Pack 3.2

October 21, 1993

Byline: Business Editors and Computer Writers

...provides scanners and other peripherals with "Colortags" -- allowing for recognition of exact color characteristics that **automatically** **correct** color deviations and produce output faithful to the **original** image.

IMAGE-IN Power Pack 3.2 and Professional Pack 3.2 consist of three enhanced productivity applications: Image **Editing**, Optical Character **Recognition** (OCR), and Raster-to-Vector conversion. The products are designed to provide users with a...

5/3,K/16 (Item 1 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2004 Business Wire. All rts. reserv.

00499243 20010416106B8961 (USE FORMAT 7 FOR FULLTEXT)
Mobile Automation 2000 Named a 2001 Finalist by Network Computing for
Well-Connected Award-Mobile Automation 2000 Enterprise Edition Tops Mobile
Device Management System for Network Category Based on its Ability to
Provide...

Business Wire

Monday, April 16, 2001 07:59 EDT

JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT

DOCUMENT TYPE: NEWSPRINT

WORD COUNT: 726

...Automated discovery and automated hardware/software inventory
(WMI, DMI, and WFM support)

- Remote event scheduling
- **Detection** and prevention of unauthorized end-user **modification** to desktops and critical configuration files
- File-gathering and distribution mechanisms
- **Automated replacement** of improperly modified files with the **original** version
- Web-based interface for diagnosing mobile system problems from anywhere, including a wireless handheld...

5/3,K/17 (Item 2 from file: 610)
DIALOG(R)File 610:Business Wire
(c) 2004 Business Wire. All rts. reserv.

00492264 20010403093B1516 (USE FORMAT 7 FOR FULLTEXT)
UGS Implements Mobile Automation 2000 for Worldwide Software Distribution and License Tracking-More than 3,500 nodes in 24 different countries easily managed from single central location

Business Wire

Tuesday, April 3, 2001 08:08 EDT

JOURNAL CODE: BW LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT

DOCUMENT TYPE: NEWSPRINT

WORD COUNT: 625

...Automated discovery and automated hardware/software inventory
(WMI, DMI and WFM support)

- Remote event scheduling
- **Detection** and prevention of unauthorized end-user **modification** to desktops and critical configuration files
- File-gathering and distribution mechanisms
- **Automated replacement** of improperly modified files with the **original** version
- Web-based interface for diagnosing mobile system problems from anywhere, including a wireless handheld...

5/3,K/18 (Item 1 from file: 613)
DIALOG(R)File 613:PR Newswire
(c) 2004 PR Newswire Association Inc. All rts. reserv.

00683311 20011130HSF001 (USE FORMAT 7 FOR FULLTEXT)

NEW Web Security Tool Stops Hackers From Modifying Websites
PR Newswire

Friday, November 30, 2001 07:02 EST

JOURNAL CODE: PR LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT

DOCUMENT TYPE: NEWSWIRE

WORD COUNT: 396

TEXT:

Cimcor, Inc. releases its new unauthorized file **change detection** system for Web Servers, CimTrak -- Web Security **Edition**. This new product **detects** unauthorized **changes** to websites and will **automatically restore** those files back to their **original** unaltered state. CimTrak -- Web Security Edition can be implemented as a stand-alone product or...

File 347:JAPIO Nov 1976-2004/Jun (Updated 041004)

(c) 2004 JPO & JAPIO

File 350:Derwent WPIX 1963-2004/UD,UM &UP=200465

(c) 2004 Thomson Derwent

Set	Items	Description
S1	155208	(DETECT??? OR NOTIC??? OR SPOT? ? OR SPOTTED OR SPOTTING OR SENS??? OR RECOGNI?) (7N) (CHANG??? OR ALTER??? OR ALTERATION? ? OR MODIF???? OR MODIFICATION? ? OR EDIT??? OR DELET??? OR ERAS??? OR REMOV??? OR RENAM??? OR VANDALISM OR DEFAC?)
S2	171110	(MASTER OR ORIGINAL OR PRIMARY OR MAIN) (10N) (REPLAC? OR RESTOR??? OR OVERWITR? OR REVERT??? OR REVERSION OR SWAP???? OR SUBSTITUT? OR SWITCH??? OR EXCHANG??? OR FIX??? OR CORRECT???)
S3	3220	S2(5N) (AUTOMAT? OR DYNAMIC? OR REAL() TIME OR BEHIND(2W) SCENE? ? OR TRANSPARENT? OR FLY)
S4	46	S1 AND S3
S5	1703	S1 AND S2
S6	1	S5 AND (WEBPAGE? ? OR (WEB OR INTERNET) () (PAGE? ? OR SITE? ?) OR WEBSITE? ?)
S7	2	S5 AND (HACK??? OR DEFAC? OR VANDALISM)
S8	142	S1:S2 AND (WEBPAGE? ? OR (WEB OR INTERNET) () (PAGE? ? OR SITE? ?) OR WEBSITE? ?)
S9	3	S8 AND (HACK??? OR DEFAC? OR VANDALISM)
S10	4	S4 AND IC=G06F
S11	8	S10 OR S6 OR S7 OR S9
S12	109	S1:S2 AND (HACK??? OR DEFAC? OR VANDALISM)
S13	24	S12 AND IC=G06F
S14	21	S13 NOT S11
S15	65	AU='FORSTER K':AU='FORSTER K T'
S16	2	S15 AND S1:S2
S17	114	S8 AND IC=G06F
S18	110	S17 NOT (S11 OR S14 OR S16)
S19	37	S18 AND AC=US/PR
S20	25	S19 AND AY=(1970:2000)/PR
S21	18	S18 AND PY=1970:2000
S22	33	S20:S21

11/5/4 (Item 1 from file: 350)
DIALOG(R) File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015933869
WPI Acc No: 2004-091710/200410
Related WPI Acc No: 2004-091689
XRPX Acc No: N04-073551

Web page protecting method involves comparing specific portions of pages with page samples in specific time interval to evaluate changes in pages for detecting hacking

Patent Assignee: HEJL P (HEJL-I)

Inventor: HEJL P

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
CA 2429503	A1	20031124	CA 2429503	A	20030526	200410 B

Priority Applications (No Type Date): CA 2387324 A 20020524

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
CA 2429503	A1	E	10 G06F-012/14	

Abstract (Basic): CA 2429503 A1

NOVELTY - The web pages to be protected are saved as samples. Specific portions of pages that are not checked, and time interval during which checking is not performed, are selected. The portions of pages other than selected portions are compared with samples in the interval other than selected interval to evaluate changes in pages to detect hacking. Changes are indicated to page owner to restore original page status.

USE - For protecting web pages from corruption that occurs due to hardware error, software bug, hacker and virus.

ADVANTAGE - Evaluates the changes in the web pages automatically and easily, thereby preventing program/data with virus pattern from being inserted into the web pages

pp; 10 DwgNo 0/1

Title Terms: WEB; PAGE; PROTECT; METHOD; COMPARE; SPECIFIC; PORTION; PAGE; PAGE; SAMPLE; SPECIFIC; TIME; INTERVAL; EVALUATE; CHANGE; PAGE; DETECT; HACK

Derwent Class: T01

International Patent Class (Main): G06F-012/14

International Patent Class (Additional): H04L-009/00; H04L-012/22

File Segment: EPI

11/5/5 (Item 2 from file: 350)

DIALOG(R) File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015875980 **Image available**
WPI Acc No: 2004-033811/200403
XRPX Acc No: N04-026892

World wide web page protection method involves detecting hacking traces and illegitimacy in web pages, after which original status of web pages is restored

Patent Assignee: HEJL P (HEJL-I)

Inventor: HEJL P

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20030221129	A1	20031127	US 2003445229	A	20030527	200403 B

Priority Applications (No Type Date): US 2003445229 A 20030527

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
US 20030221129	A1	4	G06F-012/14	

Abstract (Basic): US 20030221129 A1

NOVELTY - The world wide web (WWW) pages to-be-protected are stored as a sample. A non-compared portion of **web pages** is selected and corresponding time interval is defined. The **web pages** other than selected portions, are compared with sample outside defined interval, so as to detect **hacking** traces and illegitimacy in **web pages**. The detection result is notified to a page owner and **original** status of **web pages** is **restored**.

USE - For protecting world wide web (WWW) pages from hardware error, software bug, **hacker** and virus.

ADVANTAGE - Enables for accurate differentiation between legitimate and illegitimate changes with respect to WWW pages, automatically.

DESCRIPTION OF DRAWING(S) - The figure shows a flow diagram explaining the WWW page protection method.

pp; 4 DwgNo 1/1

Title Terms: WORLD; WIDE; WEB; PAGE; PROTECT; METHOD; DETECT; **HACK** ; TRACE ; WEB; PAGE; AFTER; ORIGINAL; STATUS; WEB; PAGE; RESTORATION

Derwent Class: T01; W01

International Patent Class (Main): G06F-012/14

International Patent Class (Additional): G06F-009/00; G06F-011/30; H04L-009/00; H04L-009/32

File Segment: EPI

11/5/6 (Item 3 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

015648430 **Image available**

WPI Acc No: 2003-710613/200367

XRPX Acc No: N03-568191

Web resources illegitimate change detecting apparatus comprises **web source protection processing sub-system**, for generating and inserting **illegitimate change detecting information**, and **web resource change detecting sub-system**

Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N); LEE J S (LEEJ-I); MOON K Y (MOON-I); PARK C H (PARK-I)

Inventor: LEE J S; MUN G Y; PARK C H; MOON K Y

Number of Countries: 002 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20030145197	A1	20030731	US 2002274996	A	20021022	200367 B
KR 2003056285	A	20030704	KR 200186482	A	20011228	200377

Priority Applications (No Type Date): KR 200186482 A 20011228

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
US 20030145197	A1	15	H04L-009/00	
KR 2003056285	A		G06F-017/00	

Abstract (Basic): US 20030145197 A1

NOVELTY - **Web resources illegitimate change detecting apparatus** comprises a **web source protection processing sub-system**, for generating and inserting **illegitimate change detecting information** into corresponding **web resource**; and a **web resource change detecting sub-system** for judging whether or not the corresponding **web resource** is **illegitimately changed**, based on the **illegitimate change detecting information**.

DETAILED DESCRIPTION - **Web resources illegitimate change detecting apparatus** comprises a **web source protection processing sub-system**, for generating and inserting **illegitimate change detecting information** into corresponding **web resource**, the **illegitimate change detecting information** being used to **detect** whether or not the **web resource** is **changed illegitimately**; and a **web resource change detecting sub-system** for judging whether or not the corresponding **web resource** is **illegitimately changed**, based on the **illegitimate change detecting information** contained in the **web resource**, when the **web resource** is executed by a **communication network**.

An INDEPENDENT CLAIM is also included for a computer-readable recording medium containing computer-executable instructions, for performing the **detection** of an illegitimate **change** of web resources.

USE - Web resources illegitimate **change** **detecting** apparatus, useful in e.g. electronic commerce services and on-line stock services.

ADVANTAGE - The illegitimate **change** **detecting** information is verified in real time when the corresponding **web page** is inquired, **detecting** the illegitimate **change** of the **web page**. The user can confirm the illegitimate change of the **web page**, by clicking the link to the illegitimate **change** **detecting** information only when necessary, obtaining an effective processing. Problems such as the manipulation of the goods price and the stock price caused by the **hacking** of the web server can be prevented.

DESCRIPTION OF DRAWING(S) - The figure is a schematic block diagram of a web resource protection processing sub-system.

pp; 15 DwgNo 2/5

Title Terms: WEB; RESOURCE; CHANGE; DETECT; APPARATUS; COMPRISE; WEB; SOURCE; PROTECT; PROCESS; SUB; SYSTEM; GENERATE; INSERT; CHANGE; DETECT; INFORMATION; WEB; RESOURCE; CHANGE; DETECT; SUB; SYSTEM

Derwent Class: T01; W01

International Patent Class (Main): G06F-017/00; H04L-009/00

File Segment: EPI

11/5/8 (Item 5 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

014613623 **Image available**

WPI Acc No: 2002-434327/200246

XRPX Acc No: N02-341839

Anti-alteration system for homepages, automatically recovers altered safe-web-file, when illegally altered safe-web-file is checked

Patent Assignee: GAO Z Y (GAOZ-I); GAO Z (GAOZ-I)

Inventor: GAO Z

Number of Countries: 002 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20020040432	A1	20020404	US 2001965968	A	20010926	200246 B
JP 2002175010	A	20020621	JP 2001161754	A	20010530	200256

Priority Applications (No Type Date): JP 2001161754 A 20010530; JP 2000299305 A 20000929

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
-----------	------	-----	----	----------	--------------

US 20020040432	A1	14		H04L-009/00	
----------------	----	----	--	-------------	--

JP 2002175010	A	10		G09C-001/00	
---------------	---	----	--	-------------	--

Abstract (Basic): US 20020040432 A1

NOVELTY - A web server in public-web-server computer checks whether the encrypted safe-web-file is illegally altered, upon receiving a user's request, and sends deciphered web-file back to user. A recovery unit encrypts web-file to safe-web-file on original-web-server computer. The public web server automatically recovers the altered safe-web-file, when the illegally altered file is checked.

USE - For prohibiting illegal alteration of homepages.

ADVANTAGE - The web file containing the altered data can be automatically replaced with the original web file, on detection of file alteration, hence the homepage can be automatically reinstated and the transmission of illegally changed data to user is prevented. The alteration prevention system can be installed without any change in current system. The financial impact is not obtained, since no special machine or technology is needed and the currently used browser application and tools can be used without burden, hence there is no impact on Internet users.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of

anti-alteration system.

pp; 14 DwgNo 2/10

Title Terms: ANTI; ALTER; SYSTEM; AUTOMATIC; RECOVER; ALTER; SAFE; WEB;
FILE; ALTER; SAFE; WEB; FILE; CHECK

Derwent Class: T01; W01

International Patent Class (Main): G09C-001/00; H04L-009/00

International Patent Class (Additional): G06F-012/00 ; G06F-012/14 ;
G06F-013/00

File Segment: EPI

14/5/3 (Item 3 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

015933848

WPI Acc No: 2004-091689/200410

Related WPI Acc No: 2004-091710

XRPX Acc No: N04-073533

World wide web (WWW) page corruption detection and correction method involves comparing currently displayed WWW pages with protected sample WWW pages, at defined time intervals

Patent Assignee: HEJL P (HEJL-I)

Inventor: HEJL P

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
CA 2387324	A1	20031124	CA 2387324	A	20020524	200410 B

Priority Applications (No Type Date): CA 2387324 A 20020524

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
CA 2387324	A1	E	9 G06F-012/14	

Abstract (Basic): CA 2387324 A1

NOVELTY - A set of protected sample world wide web (WWW) pages are stored through a browser. The currently displayed WWW pages are compared with the stored pages, at defined time intervals. If the content in the compared pages are different, **hacking** traces are searched in currently displayed pages and are changed, to **restore** the **original** status of the pages under display.

USE - For detecting and correcting corruption of static and dynamic WWW pages, due to hardware error, **hacker**, software bug and virus.

ADVANTAGE - The **original** status of the WWW pages can be **restored** efficiently, in an automated or semi-automated manner. The method is inexpensive and efficient. The WWW pages can be stored through browsers without requiring a need to access the servers.

pp; 9 DwgNo 0/1

Title Terms: WORLD; WIDE; WEB; PAGE; CORRUPT; DETECT; CORRECT; METHOD; COMPARE; CURRENT; DISPLAY; PAGE; PROTECT; SAMPLE; PAGE; DEFINE; TIME; INTERVAL

Derwent Class: T01

International Patent Class (Main): G06F-012/14

International Patent Class (Additional): G06F-011/00 ; H04L-009/00; H04L-012/26

File Segment: EPI

14/5/6 (Item 6 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

015608367 **Image available**

WPI Acc No: 2003-670524/200363

XRPX Acc No: N03-535365

Intrusion detection method using adaptive rule estimation in network-based intrusion detection system, involves estimating changed position of packet collected on network from original rule

Patent Assignee: ELECTRONICS & TELECOM RES INST (ELTE-N); KOREA ELECTRONICS & TELECOM RES INST (KOEL-N); CHOI B C (CHOI-I); PARK C H (PARK-I); SEO D I (SEOD-I); SOHN S W (SOHN-I)

Inventor: CHOI B C; PARK C H; SEO D I; SON S W; SOHN S W; SUH D I

Number of Countries: 002 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20030115486	A1	20030619	US 2002273140	A	20021018	200363 B
KR 2003049078	A	20030625	KR 200179179	A	20011214	200373
KR 427449	B	20040414	KR 200179179	A	20011214	200453

Priority Applications (No Type Date): KR 200179179 A 20011214

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
US 20030115486	A1	7	G06F-011/30	
KR 2003049078	A		H04L-012/22	
KR 427449	B		H04L-012/22	Previous Publ. patent KR 2003049078

Abstract (Basic): US 20030115486 A1

NOVELTY - A packet is collected on a network and an original rule that is most similar to the collected packet is searched from a rule database (30) in which a rule for intrusion **detection** is stored. The **changed** position of the collected packet is estimated from the original rule so as to determine whether a **hacker** intrudes.

USE - For detecting intrusion of **hacker** on computer network by using adaptive rule estimation in network-based intrusion detection system (NIDS).

ADVANTAGE - Enables preventing the indirect attack of the **hacker** using packet whose number of bits is changed due to deletion/insertion of characters from/into the packet.

DESCRIPTION OF DRAWING(S) - The figure shows a flowchart illustrating the intrusion detection method by adaptive rule estimation in NIDS.

rule database (30)
pp; 7 DwgNo 2/6

Title Terms: INTRUDE; DETECT; METHOD; ADAPT; RULE; ESTIMATE; NETWORK; BASED ; INTRUDE; DETECT; SYSTEM; ESTIMATE; CHANGE; POSITION; PACKET; COLLECT; NETWORK; ORIGINAL; RULE

Derwent Class: T01

International Patent Class (Main): G06F-011/30 ; H04L-012/22

File Segment: EPI

14/5/7 (Item 7 from file: 350)

DIALOG(R) File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015552547 **Image available**
WPI Acc No: 2003-614702/200358

Unified security management system

Patent Assignee: IGLOO SECURITY INC (IGLOO-N)

Inventor: CHA S G; JU J H; JUN B H; LEE Y G; PARK G H; PARK H T

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
KR 2003035143	A	20030509	KR 200167074	A	20011030	200358 B

Priority Applications (No Type Date): KR 200167074 A 20011030

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
KR 2003035143	A	1	G06F-015/00	

Abstract (Basic): KR 2003035143 A

NOVELTY - A unified security management system is provided to normalize event logs, generated by various **hacking** detection systems, into mapping event logs by using a mapping table reclassified according to a detection type and a risk degree.

DETAILED DESCRIPTION - The system comprises an agent(10), a manager(20), and a user interface. The agent(10) includes a collector, a storage, and a controller. The collector collects event logs from **hacking** detection systems. The storage stores a mapping table reclassified according to a **hacking** detection type and a risk degree. The controller normalizes the collected event logs into mapping event logs by comparing the collected event logs with the mapping table. The manager receives the normalized mapping event logs, analyzes them, generates corresponding messages according to an analysis result, and transmits the corresponding messages to a console. The user interface analyzes the corresponding messages transmitted from the manager(20), outputs the analyzed corresponding message, and adds or **modifies** the

hacking detection types. If the mapping event log has a low risk, the manager outputs a simple event message as the corresponding message, but if the mapping event log has a high risk, the manager outputs an alarm event message as the corresponding message.

pp; 1 DwgNo 1/10

Title Terms: UNIFIED; SECURE; MANAGEMENT; SYSTEM

Derwent Class: T01

International Patent Class (Main): G06F-015/00

File Segment: EPI

14/5/8 (Item 8 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

015407487

WPI Acc No: 2003-469625/200345

XRPX Acc No: N03-373575

System and method for ensuring computer host safety

Patent Assignee: DONGWEICHENG SCI TECHNOLOGY CO LTD (DONG-N)

Inventor: CHEN Y; LIANG Z

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
CN 1405686	A	20030326	CN 2001142167	A	20010914	200345 B

Priority Applications (No Type Date): CN 2001142167 A 20010914

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
CN 1405686	A		G06F-012/14	

Abstract (Basic): CN 1405686 A

NOVELTY - The various protection measures in hardware and in software are utilized in the method in order to prevent the **hacker** 's intruding and protect the safety of the data on the hard disc. In the software, the computer is allowed to start up only the fingerprint authentication is passed or the IC card is utilized. The authentication is done before the computer starts up. In the hardware, the safety of the data on the hardware is protected by use of the encryption/decryption cards and the micro **switch** on the case. The system at least includes the computer **main** board, the processor, the north bridge chip, the south chip, the I/O control chip, the keyboard, the card reader, the fingerprint scanner, the hardware, the encryption/decryption card and the case.

DwgNo 0/0

Title Terms: SYSTEM; METHOD; ENSURE; COMPUTER; HOST; SAFETY

Derwent Class: T01; T04; T05

International Patent Class (Main): G06F-012/14

International Patent Class (Additional): G06F-009/445 ; G06F-012/16

File Segment: EPI

14/5/11 (Item 11 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

014917433

WPI Acc No: 2002-738140/200280

Data shield

Patent Assignee: GYE Y J (GYEY-I)

Inventor: GYE Y J

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
KR 2002044452	A	20020615	KR 200073867	A	20001206	200280 B

Priority Applications (No Type Date): KR 200073867 A 20001206

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes
KR 2002044452 A G06F-012/16

Abstract (Basic): KR 2002044452 A

NOVELTY - A data shield is provided to build a stable computer environment, to save time and cost, and to stably apply a computer system by restraining the change or deletion of the folders and the data in a computer.

DETAILED DESCRIPTION - A data shield is developed by using a C++ program language. Upon installing a program, the folder composition, the file structure and composition and the user environment set-up of a user PC(Personal Computer) are memorized. The user PC environment is compared to a first set-up environment in real time. If a wrong operation, **hacking** or virus infection is sensed, the first set-up environment is restored. The files and folders are restrained from a random movement, deletion and change. If a program undesired by a manager is **sensed**, the program is **removed** immediately.

DwgNo 0/0

Title Terms: DATA; SHIELD

Derwent Class: T01

International Patent Class (Main): G06F-012/16

File Segment: EPI

14/5/13 (Item 13 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

014856073 **Image available**

WPI Acc No: 2002-676779/200273

XRPX Acc No: N02-535002

Management of data storage capacity e.g. for headless computer entities, where the computer entity stores a license data describing limitations on usage of the data storage device in a storage region outside the logical disk area

Patent Assignee: HEWLETT-PACKARD CO (HEWP)

Inventor: GOLD S

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
GB 2372347	A	20020821	GB 20014103	A	20010220	200273 B

Priority Applications (No Type Date): GB 20014103 A 20010220

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes
GB 2372347 A 39 G06F-001/00

Abstract (Basic): GB 2372347 A

NOVELTY - Headless computer entity is provided with a license key data stored on a raw disk sector separate from a system disk and a data disk. The license key data is used to control the available data storage capacity within the headless computer entity, and protect the computer entity from unauthorized upgrade to a higher product specification. The license key data is encrypted and protected from **hacking** via software updates introduced on an external data carrier such as CD ROM.

DETAILED DESCRIPTION - INDEPENDENT CLAIM included for the following:

- (a) physical data storage device;
- (b) method of operating a computer entity;
- (c) method of generating a computer entity

USE - For headless computer entities.

ADVANTAGE - The license key data may ensure that users cannot add a pre-formatted extra disk to a computer entity, and thereby gain extra data storage capacity, without reference back to the manufacturer. The license key data ensures that after a physical disk **replacement**, a headless computer entity is still restricted to use an **original** number and capacity of logical disk, so if a user **replaces** a physical

disk with a larger capacity physical disk, then only the original authorized data capacity specified by the license key data will be used on the replacement physical disk. This has the added benefit that computer entity tape back-ups will be compatible with any past and future computer entities, regardless of the size of the physical hardware disk, since the actual logical data partition stored on the back-up tape will always be the same size.

DESCRIPTION OF DRAWING(S) - The diagram shows a license key data stored in a raw disk area of a data storage device of the headless computer entity.

pp; 39 DwgNo 5/13

Title Terms: MANAGEMENT; DATA; STORAGE; CAPACITY; HEAD; COMPUTER; ENTITY; COMPUTER; ENTITY; STORAGE; LICENCE; DATA; DESCRIBE; LIMIT; DATA; STORAGE; DEVICE; STORAGE; REGION; LOGIC; DISC; AREA

Derwent Class: T01

International Patent Class (Main): G06F-001/00

File Segment: EPI

14/5/21 (Item 21 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

008483211 **Image available**

WPI Acc No: 1990-370211/199050

XRPX Acc No: N90-282274

Program data checking system - includes use of algorithm producing known signature to check validity of program prior to use

Patent Assignee: BULL CP8 (SELA)

Inventor: OISEL A; UGON M

Number of Countries: 018 Number of Patents: 010

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 402210	A	19901212	EP 90401476	A	19900601	199050	B
WO 9015384	A	19901213				199101	
FR 2647924	A	19901207				199105	
JP 3503220	W	19910718	JP 90508410	A	19900601	199135	
CA 2034002	C	19950523	CA 2034002	A	19900601	199528	
US 5442645	A	19950815	US 91646638	A	19910226	199538	
			US 94328963	A	19941024		
EP 402210	B1	19950830	EP 90401476	A	19900601	199539	
DE 69021935	E	19951005	DE 621935	A	19900601	199545	
			EP 90401476	A	19900601		
ES 2079457	T3	19960116	EP 90401476	A	19900601	199610	
KR 9409699	B1	19941017	KR 91700143	A	19910206	199636	

Priority Applications (No Type Date): FR 897429 A 19890606

Cited Patents: 2.Jnl.Ref; DE 3709524; EP 280035

Patent Details:

Patent No	Kind	Lan	Pg	Main	IPC	Filing Notes
-----------	------	-----	----	------	-----	--------------

EP 402210	A					
		Designated States (Regional):		AT BE CH DE ES FR GB GR IT LI LU NL SE		
WO 9015384	A					
		Designated States (National):		CA JP KR US		
CA 2034002	C	F		G06F-011/08		
US 5442645	A	15	G01R-031/28	Cont of application US 91646638		
EP 402210	B1	F	20	G06F-011/08		
		Designated States (Regional):		AT BE CH DE DK ES FR GB GR IT LI LU NL SE		
DE 69021935	E			G06F-011/08	Based on patent EP 402210	
ES 2079457	T3			G06F-011/08	Based on patent EP 402210	
KR 9409699	B1			G06F-011/08		

Abstract (Basic): EP 402210 A

In order to verify the integrity of a data message or logic signal, and algorithm (A) is applied to at least part of the original message and a signature (S1, S2,..Sm) is calculated and memorised. The equipment also includes the processing circuits (11) capable of applying the algorithm.

In order to verify the integrity of the message at the point of use, the algorithm is again applied, and the signature determined. This is then compared with that determined from the original message.

USE - The system allows checking of a program in order to ensure that no accidental or deliberate alteration of the program has occurred. (19pp Dwg.No.3/6)

Title Terms: PROGRAM; DATA; CHECK; SYSTEM; ALGORITHM; PRODUCE; SIGNATURE; CHECK; VALID; PROGRAM

Derwent Class: T01

International Patent Class (Main): G01R-031/28; G06F-011/08

International Patent Class (Additional): G06F-009/06 ; G06F-012/16 ; H04L-009/00

File Segment: EPI

09757493 SUPPLIER NUMBER: 19801148 (THIS IS THE FULL TEXT)
Seiko Instruments Signs Joint Development Pact With CYBER VISTA, Silicon Valley Software Developer; Firms to Build Specific Application "Agents" For Use In Future SIU Products.

Business Wire, p9300050

Sep 30, 1997

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 532 LINE COUNT: 00053

TEXT:

SAN JOSE, Calif.--(BUSINESS WIRE)--Sept. 30, 1997--Seiko Instruments USA Inc. (SIU), a leading provider of innovative products designed to solve business and home/office problems and enhance productivity, Tuesday announced a joint development agreement with CYBER VISTA, a growing supplier of intranet and Internet-based "smart agent" software.

Terms of the agreement were not disclosed.

CYBER VISTA, creator of unique Information Task Management (ITM) software, will begin immediately to develop its "Data Grabber task agents" for custom use in SIU's business and consumer product applications. Specific products and release dates will be provided in the future.

According to Sreenath Pendyala, vice president and general manager of SIU, the primary focus of the agreement is on "Data Grabber" technology that allows intranet and Internet users to request and get immediate access to online information.

"Seiko Instruments wants to provide customers with Internet-ready products to enhance productivity," Pendyala said. "This joint development project will result in unique technology that will benefit all PC users."

"Seiko Instruments is an ideal partner because of its markets, and adaptability of our task agents," said Daniel Ashby, CYBER VISTA president. "This project will make the power and control of Data Grabber quickly available to consumers and members of the business community."

He added that "webcasting" and "push" technologies provide customized information, but do not deal with source environment, format and destination environment issues. "CYBER VISTA's Internet/intranet Information Task Management (ITM) software addresses all of these issues, runs unattended and is customized to each application."

The technology involves "find" and "deliver" segments. The "find" side can locate, collect, extract and analyze information as specified by the user. The "deliver" capabilities include processing, reformatting and providing the information in the format or environment the user requested.

CYBER VISTA, based in San Mateo, Calif., produces and markets powerful, easy-to-use management software to find, monitor, compare, analyze, retrieve, reformat and distribute user-specified online information. In addition to retrieving ("grabbing") data, the company's software makes that information useable and delivers it automatically.

The ITM core technology adapts reusable components and engines for client/server applications to create scaleable information processing and distribution solutions. Phone: 415/372-0800. Web site:

<http://www.cybervista.com> .

Seiko Instruments USA, a privately held U.S. corporation, is the Western Hemisphere marketing and sales affiliate of Seiko Instruments Inc., one of three worldwide Seiko group companies. With the focus on providing "big technology in small packages," SIU products include electronic components, micro thermal printers, factory automation robotics systems, color printers and supplies, consumer electronic products, digital imaging and compact convenient peripherals for the office and home/office personal computer market.

SIU has headquarters at 1130 Ringwood Court, San Jose, Calif. 95131. Telephone: 408/922-5900, Fax: 408/433-3261, Web site:
<http://www.seikosmart.com> . -0-

Editor/Analyst Note: For photos, interviews or further information,

contact Les Goldberg Public Relations or Brough Communications.

CONTACT: Les Goldberg Public Relations

Les Goldberg, APR, 714/545-3117

Fax: 714/545-1197

lgpr@pacbell.net

or

Brough Communications

Bruce Brough, 408/430-0100

Fax: 408/438-0204

bruce@brough.com

COPYRIGHT 1997 Business Wire

COMPANY NAMES: Cyber Vista--Product development; Seiko Instruments USA
Inc.--Product development

INDUSTRY CODES/NAMES: BUS Business, General; BUSN Any type of
business

DESCRIPTORS: Computer software industry--Product development

PRODUCT/INDUSTRY NAMES: 7372681 (Internet Access Software)

SIC CODES: 7372 Repackaged software

FILE SEGMENT: NW File 649

?

DIALOG(R) File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0773785 BW0020

CYBER VISTA: CYBER VISTA Offers Free Download of New Data Grabber Lite, Leading-Edge Software for Information Task Management

November 17, 1997

Byline: Business Editors/Computer Writers
Dateline: SAN MATEO, Calif.
Time: 03:00 PT
Word Count: 494

See CYBER VISTA at Microsoft's COMDEX Pavilion

SAN MATEO, Calif.--(BUSINESS WIRE)--Nov. 17, 1997--
Unattended 'Task Agents' Monitor Web Sites, Track Stocks,
Find Lowest Air Fares, or Demo Windows APIs,
Then Automatically Notify User or Take 'Scripted' Action
CYBER VISTA, San Mateo-based developer of Intra/Internet
Information Task Management (ITM) software used by major
organizations including the U.S. government, Seiko Instruments
America (SIU), The Sabre Group and TCI, will demonstrate a new "Lite"
version at COMDEX available immediately as a free download from the
company's Internet home page (www.cybervista.com).

"Data Grabber Player Lite includes four customized "task
agents" and a demonstration, so individuals can learn and apply
useful internet applications immediately and at no cost," said
Daniel Ashby, CYBER VISTA president. "Although our current focus is
major corporate applications, end users need this introduction to ITM
technology, since we plan to sell more robust upgraded versions on
the Internet for \$99 from January 1 throughout the first quarter of
1998."

DG Player Lite will let users try regular Data Grabber
functionality in at least four useful and proven applications. All
task agents allow users to make individual choices, and run
unattended. They can:

- Retrieve and present lowest air fare at user-specified date and
time;
- Monitor any web site for changes;
- Monitor web site for unauthorized changes, then automatically
alert user and restore site;
- Track any five selected stocks, then alert user to major changes
on desktop; and
- Demonstrate Windows APIs for technical users.

All of these "Lite" applications are already user proven by
individuals and corporations, including Seiko Instruments America,
TCI and Sabre Group's Travelocity.

"This free product is the first widely-available answer to cries
from industry editors and analysts for a way to make the mushrooming
volume of information or 'knowledge' both accessible and useful,"
said Nick Roche, CYBER VISTA vice president, sales and marketing.
"Earliest applications, and some soon to be announced do just that --
they make on-line information manageable."

About CYBER VISTA:

CYBER VISTA, based in San Mateo, Calif., produces and markets
powerful, easy-to-use management software to find, monitor, compare,
analyze, retrieve, reformat and distribute user-specified on-line
information. In addition to retrieving ("grabbing") data, this
software makes that information useable, and delivers it
automatically in a wide range of environments (cell phone, beeper,
e-mail, desktop, etc.).

The ITM core technology adapts reusable components and engines for client/server applications to create scaleable information processing and distribution solutions. It has both "find" and "deliver" segments. The "find" side locates, collects, extracts and analyzes user specified information. "Deliver" includes processing and "repurposing" data. Phone: (415) 372-0800. Website: <http://www.cybervista.com>.

Editors and Industry Analysts: For further information, interviews, or photographs contact Brough Communications.

CONTACT: Brough Communications
Bruce Brough/ Marsha Keeffer/ Christian Tacy
Tel: 408/430-0100
Fax: 408/438-0204
Email: bruce@brough.com
marsha@brough.com
christian@brough.com

KEYWORD: CALIFORNIA NEVADA

INDUSTRY KEYWORD: COMPUTERS/ELECTRONICS COMED

INTERACTIVE/MULTIMEDIA/INTERNET PRODUCT TRADESHOW

Today's News On The Net - Business Wire's full file on the Internet with Hyperlinks to your home page.

URL: <http://www.businesswire.com>

>
?

DIALOG(R) File 810:Business Wire
(c) 1999 Business Wire . All rts. reserv.

0746157 BW1667

TCI INTESSERA: TCI Intessera Division to Use CYBER VISTA Data Grabber Maximizer for Website Information Security Management; Customized System 'Task Agents' Alert Webmasters to Attempted Intrusion

September 15, 1997

Byline: Business Editors & High Tech Writers
Dateline: SAN MATEO, Calif.
Time: 17:15 PT
Word Count: 314

SAN MATEO, Calif.--(BUSINESS WIRE)--Sept. 15, 1997--CYBER VISTA, a San Mateo-based developer of Information Management Technology (ITM) software solutions, announced TCI's Intessera Division as a major customer for CYBER VISTA's Data Grabber Maximizer System.

Intessera provides customized computer applications for government and corporate clients worldwide.

Intessera will customize web "sentinels" to inform webmasters of attempted intrusions or changes and to archive web history with CYBER VISTA task agents. "Initially, we are targeting government customers. We'll leverage that activity beyond government into selected vertical industries," said Eric Kemp, manager and systems administrator for Intessera's technology group.

"Data Grabber can detect virtually any change to a website, including text, HTML, graphics and more. Other packages we've tried just can't do that," he said. "The Data Grabber Maximizer System is a wonderful application development environment robust enough to meet every customer need."

Daniel Ashby, co-founder and president of CYBER VISTA, said, "Intessera has demonstrated a forward thinking application of Data Grabber Maximizer technology, which can continuously monitor all or part of a web site for unauthorized changes, and 'report' automatically."

CYBER VISTA, based in San Mateo, produces and markets powerful, easy-to-use on-line information management software to find, monitor, compare, analyze, retrieve, reformat, and distribute on-line information as specified by the user. Years of research and development have resulted in CYBER VISTA's unique Intra/Internet Information Task Management (ITM) technology -- a powerful and easy to use solution for on-line information management.

CYBER VISTA's core technologies include reusable components and engines for client/server applications, providing scaleable solutions for information processing and distribution.

Note to Editors and Industry Analysts: For further information, interviews, or photographs contact Brough Communications.

CONTACT: Brough Communications
Bruce Brough, Marsha Keeffer, Christian Tacy, 408/430-0100
bruce@brough.com
marsha@brough.com
christian@brough.com

KEYWORD: CALIFORNIA

INDUSTRY KEYWORD: COMPUTERS/ELECTRONICS COMED
INTERACTIVE/MULTIMEDIA/INTERNET PRODUCT
Today's News On The Net - Business Wire's full file on the Internet with Hyperlinks to your home page.

URL: <http://www.businesswire.com>

>
?